



IBRAHIM BADAMASI BABANGIDA UNIVERSITY, LAPAI



UNIVERSITY ARTIFICIAL INTELLIGENCE POLICY

September 2026

SECTION ONE: INTRODUCTION

1.1 Policy Statement

Ibrahim Badamasi Babangida University, Lapai (IBBU) shall govern the use, development, procurement and deployment of artificial intelligence (AI) in a manner that protects human agency, academic and research integrity, privacy, security, equity, safety, accountability and public trust while enabling legitimate educational, research, administrative and institutional purposes.

AI may assist human work, but responsibility for academic, professional, research and institutional decisions shall remain with an identifiable human decision-maker. The University shall adopt a risk-based, technology-neutral and adaptable approach so that this Policy remains applicable as AI systems and capabilities change.

1.2 Authority and Legal Relationship

This Policy is a University-wide policy approved by Senate and shall be administered through the University's established governance structures and procedures.

This Policy shall be read together with the University's Statutes, Regulations, academic integrity and misconduct procedures, research ethics requirements, staff regulations, information-security requirements and other applicable University instruments.

Nothing in this Policy authorizes conduct prohibited by applicable Nigerian law, regulatory requirements, professional standards, contractual obligations or binding University rules. Where a legal, regulatory or professional requirement is more stringent than this Policy, the more stringent requirement shall apply.

The University shall maintain this Policy in alignment with applicable Nigerian data-protection law, relevant guidance of competent authorities, applicable National Universities Commission (NUC) requirements, and professional or regulatory obligations governing particular disciplines.

1.3 Purpose

The purposes of this Policy are to:

- establish clear University-wide requirements for responsible AI use;
- protect the University's academic, research and professional mission;
- promote AI literacy and responsible innovation;
- protect personal, confidential, restricted, unpublished and sensitive information;
- ensure that AI-enabled activities are proportionate to their risks and impacts;
- provide equitable access where AI is required for learning or assessment;

- establish accountability for institutional AI systems and AI-assisted decisions; and
- provide governance arrangements for monitoring, review and adaptation as AI capabilities evolve.

1.4 Scope

This Policy applies to all students, academic staff, researchers, professional and administrative staff, contractors, visiting scholars, affiliated researchers, University units and other persons acting on behalf of or using University resources for University activities.

It applies whenever AI is used in teaching, learning, assessment, research, student services, administration, communications, institutional decision-making, University business or other University activities.

Personal AI use outside University activities is outside the substantive scope of this Policy; however, University information, personal data, confidential information, intellectual property, research material and restricted information shall not be disclosed to an AI service merely because the activity is conducted using a personal device or account.

The Policy is technology-neutral and applies to generative AI, predictive AI, machine-learning systems, recommender systems, computer-vision systems, autonomous or agentic AI, AI-enabled software, synthetic media and future AI systems that perform materially similar functions.

1.5 Definitions

Artificial Intelligence (AI): A machine-based system capable of generating predictions, recommendations, content or decisions for defined objectives.

Generative AI: AI capable of generating text, code, images, audio, video or other content in response to inputs.

Predictive AI: AI that analyses historical and/or current data to identify patterns and generate predictions, forecasts, probabilities, risk estimates, or other assessments about future events, behaviours, outcomes, or conditions.

Agentic AI: An AI-enabled system capable of planning and executing multi-step actions, interacting with external systems or making decisions with limited continuous human direction.

AI-assisted work: Work in which AI contributes to a task while a human remains responsible for the reasoning, verification and final product.

High-impact AI: AI used in a decision or process that can materially affect admission, grades, scholarships, discipline, employment, health, safety, progression or other significant rights or interests.

AI literacy: The knowledge, skills, judgement and ethical awareness required to understand, use, evaluate, question and govern AI.

Material AI use: AI use that makes a substantive contribution to the content, analysis, coding, decision, product or process for which a person or University unit is accountable.

AI disclosure: A clear statement identifying material AI assistance, the tool or service used, and the nature of its contribution.

AI Register: The University's controlled record of institutional AI systems, including their owners, purposes, risk classifications, data categories, safeguards, approvals and review dates.

1.6 Foundational Principles

1.6.1 Human agency and accountability

AI may assist; accountable humans shall decide. No University process shall transfer responsibility for a decision to an AI system.

1.6.2 Purpose before technology

AI shall be used only for a legitimate educational, research, administrative or public-interest purpose and where the use is justified in relation to available alternatives.

1.6.3 Integrity and authenticity

Every person remains responsible for work submitted, published, communicated or acted upon in their name. AI shall not be used to conceal the absence of required learning, scholarship or professional competence.

1.6.4 Transparency and traceability

Material AI use shall be disclosed where required. Institutional AI systems shall have an identifiable owner, defined purpose, documented data categories, risk assessment and review record.

1.6.5 Privacy and data protection

AI use shall comply with applicable Nigerian data-protection law and University information-security requirements. Data minimisation and privacy-protective design shall be applied to institutional deployments.

1.6.6 Fairness and non-discrimination

AI use shall be assessed for material discriminatory effects, accessibility barriers, linguistic bias and other inequitable outcomes.

1.6.7 Equity of access

Where AI is required for learning or assessment, the University shall provide an institutional route that does not unfairly disadvantage persons who cannot access the technology privately.

1.6.8 Safety and proportionality

Controls shall be proportionate to the potential harm and significance of the AI use. Higher-risk uses shall require stronger controls.

1.6.9 Human-centred education

AI literacy shall strengthen critical thinking, judgement, creativity, communication and disciplinary competence rather than mere tool operation.

1.6.10 Academic freedom and professional autonomy

Within University rules and approved programme requirements, academic staff retain authority to determine pedagogically appropriate AI use in their courses.

1.6.11 Sustainability

Material AI procurement and deployment decisions shall consider energy, compute, environmental and lifecycle implications where relevant.

1.6.12 Continuous learning

The University shall maintain an adaptive governance process through which operational guidance, controls and approved-tool arrangements can be reviewed as evidence, law and technology change.

SECTION TWO: GOVERNANCE

2.1 Risk-Based AI Governance

AI use shall be classified before institutional deployment. For ordinary coursework, the applicable assessment permission category shall be established before the assessment is undertaken. Controls shall increase with the potential impact of the AI use.

Level	Description / Examples	Minimum controls
Level 1: Low	Grammar support, brainstorming, generic tutoring and non-sensitive administrative drafting.	Normal University or course rules; human verification; no confidential or restricted data.
Level 2: Moderate	AI-supported assessment, analysis of non-sensitive research data, student-support chatbots and workflow automation.	Named owner; stated purpose; human review; privacy check; disclosure or recording where required.
Level 3: High	AI affecting admissions screening, scholarships, progression, staff recruitment, sensitive research, health-related support or disciplinary recommendations.	Formal impact assessment; UAIGC approval; identifiable human decision-maker; appeal route; monitoring; security and privacy controls.
Level 4: Prohibited by default	Fully automated high-stakes decisions, covert surveillance, AI fabrication of research, unauthorised processing of sensitive personal data, or systems that cannot provide adequate accountability for their intended use.	Prohibited unless expressly authorised by Senate following documented necessity, safeguards, accountability arrangements and legal/regulatory review.

2.2. Governance Structure

2.2.1 University AI Governance Committee

A standing University AI Governance Committee (UAIGC) shall oversee implementation of this Policy.

The Committee shall comprise:

- Deputy Vice-Chancellor (Academic), Chair;
- Registrar or nominee;
- Coordinating Director of Research/Innovation or nominee;
- Director of ICT;
- **Data Protection Officer;**
- Representative of Library/Information Services;
- Representative of Quality Assurance;

- Representative responsible for Research Ethics/Integrity;
- legal representative;
- Two academic representatives from different disciplines;
- One student representative;
- One disability/inclusion representative; and
- A member with appropriate cybersecurity expertise.

The UAIGC shall:

- maintain the University's AI governance framework and risk register;
- approve or recommend approval of institutional AI systems according to their risk level and delegated authority;
- issue and maintain University-wide AI guidance, templates and approved-tool arrangements;
- review AI-related academic integrity, privacy, safety, security and discrimination incidents at governance level;
- coordinate annual AI readiness and impact reviews;
- authorise controlled AI pilots within its delegated authority;
- maintain horizon-scanning arrangements for emerging AI systems and capabilities; and
- submit an annual report on AI governance to Senate, excluding confidential case information.

2.2.2 AI Secretariat

An operational AI Secretariat shall support the UAIGC. The function may be assigned to an existing University unit where this avoids unnecessary duplication of administrative structures.

2.2.3 Faculty/College AI Leads

Each Faculty or College shall designate an AI Lead or Liaison responsible for discipline-specific guidance, staff development, assessment review and escalation of AI-related issues.

2.2.4 Institutional AI system ownership

Every institutional AI deployment shall have a named business owner and technical owner. An ownerless or unidentified AI system shall not be used for University business.

SECTION THREE: ARTIFICIAL INTELLIGENCE IN ACADEMIC PRACTICE

3.1 Teaching, Learning and Assessment

The University shall regulate student AI use at the course and assessment level according to learning outcomes and assessment requirements. A blanket University-wide prohibition or blanket permission shall not replace assessment-specific instructions.

3.1.1 Course requirements

1. Every course syllabus shall contain an explicit statement on AI use before the first major assessment.
2. Assessment instructions shall state the applicable AI permission category where different assessments have different requirements.
3. Students shall not be penalised for AI use that is expressly permitted and complies with the stated conditions.
4. Where AI use is required, the University shall provide or designate an equitable access route.
5. Where AI is prohibited for a learning outcome, the assessment shall be designed and administered so that the prohibition is meaningful.
6. Students remain responsible for the accuracy, originality, citations, reasoning and final form of submitted work.

3.1.2 AI assessment permission categories

Category		Meaning	Typical use	Student requirements
A	No AI	AI is not permitted for the assessment or specified part.	Invigilated examination; foundational skill demonstration; oral competence check.	Do not use AI; comply with assessment conditions.
B	Assistive AI	AI may assist peripheral processes but may not generate the substantive intellectual work being assessed.	Grammar, accessibility, brainstorming, planning or limited feedback.	Follow stated limits; disclose where required.
C	Collaborative AI	AI may materially assist the work as part of the learning activity.	Draft critique, coding support, data exploration or scenario analysis.	Disclose AI use; preserve relevant process evidence; verify outputs.
D	AI-integrated	AI use is itself part of the intended learning outcome.	Prompt evaluation, AI-assisted professional tasks, model critique or AI system design.	Use specified tools; document material process; critically evaluate outputs.

Where an assessment instruction is silent on AI use, the student shall seek clarification from the course lecturer before using AI. Silence shall not be treated as a substitute for clear assessment instructions.

3.3.3 Assessment design

1. Programmes shall use a balanced range of assessment methods appropriate to their learning outcomes.
2. Where independent mastery is being assessed, programmes may use secure examinations, supervised practicals, demonstrations, viva/oral examinations, observed performances or equivalent evidence of individual competence.
3. Where AI competence is a learning outcome, assessments shall require students to use, critique, verify or reflect on AI as specified by the assessment.
4. Where appropriate, assessment may include drafts, design journals, reasoning records, oral defense, source trails or reflection as evidence of process.
5. Assessment design may use authentic local problems, field data, community contexts and course-specific materials where these improve validity.
6. AI detection scores shall not be treated as conclusive evidence of academic misconduct.

3.3.4 Academic staff use of AI

1. Academic staff may use approved AI for lesson planning, brainstorming, language editing, formative feedback and other legitimate activities, subject to verification.
2. Academic staff shall not delegate final academic judgement, grading, progression decisions or disciplinary determinations to AI.
3. Confidential student work shall not be uploaded to public AI systems without an approved legal, privacy and security basis.
4. Where AI materially generates teaching materials or feedback and disclosure is necessary to maintain transparency and academic responsibility, the staff member shall disclose the material use to affected students.

3.4 Student AI Literacy

AI literacy shall be treated as a graduate capability and shall be developed through University-wide foundational learning and discipline-specific integration.

Foundation: Explain what AI and generative AI can and cannot do; understand hallucination, bias, privacy, copyright, academic integrity and disclosure.

Applied: Use AI appropriately for learning; verify outputs; compare AI-generated information with authoritative sources; document material AI assistance.

Disciplinary: Evaluate AI against the methods, evidence requirements, professional standards and ethical obligations of the relevant discipline.

Advanced/Creator: Where relevant to the discipline, design, test, audit or govern AI systems.

3.5 Research and Scholarship

1. Researchers remain responsible for research questions, methods, data, analysis, interpretation and conclusions when AI is used.
2. AI may be used for legitimate research activities such as literature discovery, coding, transcription, preliminary categorization, language editing and hypothesis brainstorming where methodologically appropriate.
3. AI shall not be used to fabricate, manipulate, selectively invent or falsely represent data, citations, quotations, participants, images, results or sources.
4. Material AI use shall be documented sufficiently to support transparency and reproducibility.
5. Confidential peer-review material, identifiable participant data, unpublished proprietary data and restricted datasets shall not be provided to AI tools unless expressly authorized.
6. AI systems shall not be listed as authors of scholarly work. Human authors shall satisfy the authorship requirements of the relevant journal, publisher, funder and professional body.
7. Researchers shall comply with applicable journal, funder, professional, regulatory and University requirements concerning AI disclosure and use.

3.5.1 Research ethics

Use of AI does not remove the requirement for Research Ethics Committee or other applicable ethics approval. Research involving AI and human participants shall address privacy, informed expectations, bias, explainable, potential harms and the consequences of automated or AI-assisted decisions.

SECTION FOUR: INFORMATION SECURITY AND PRIVACY

4.1 Data Protection, Privacy and Information Security

1. AI use shall comply with the Nigeria Data Protection Act 2023, applicable guidance of the Nigeria Data Protection Commission and University information-security requirements.
2. Student records, staff records, health information, examination materials, unpublished research data, passwords, security information and other restricted information shall not be entered into public AI services unless expressly authorised.
3. Only the minimum information necessary for an approved purpose shall be provided to an AI system.
4. A privacy and security assessment shall be completed before institutional deployment of AI that processes personal or confidential data.
5. Institutional AI procurement and deployment shall assess cross-border data transfers, vendor retention, model-training terms, deletion, access controls, encryption and incident-response arrangements.
6. The University shall maintain an inventory of AI systems that process University data.
7. A human route shall be available for data-subject requests, complaints and decisions affecting rights or significant interests.
8. Where applicable, data-subject rights and requirements relating to automated decision-making shall be implemented through the University's Data Protection Office and existing procedures.

SECTION FIVE: RESPONSIBLE AI IN ADMINISTRATION AND ACCOUNTABILITY

5.1 Procurement and Deployment of Institutional AI

An AI tool shall not become an institutional University system merely because an individual has purchased a subscription or identified a useful application. Institutional adoption shall follow documented due diligence and the University's procurement and approval requirements.

Assessment area	Minimum question
Purpose	What legitimate University problem or objective does the AI system address?
Necessity	Can the objective be achieved through a lower-risk method?
Data	What data enters the system, and is it personal, confidential, sensitive, copyrighted or unpublished?
Vendor	Who operates the system, where is data processed, and can vendor training use be controlled?
Security	Are authentication, encryption, access control, logging and incident-response controls adequate?
Accuracy	What is the known error profile and how will outputs be verified?
Bias and equity	Could different groups experience materially different outcomes or barriers?
Human oversight	Who reviews decisions and can a person override the system?
Appeal	Can an affected person challenge or correct an AI-assisted decision?
Continuity	What happens if the vendor changes price, model, terms or discontinues the service?
Exit	Can the University retrieve or delete its data and migrate to another system?
Sustainability	Are compute, energy and lifecycle implications proportionate to the intended benefit?

5.2 AI in University Administration

Low-risk administrative automation may be used where approved and appropriately controlled. AI shall not be the final decision-maker in high-impact University decisions.

The following may be used in principle, subject to approval and applicable controls:

- a) document drafting;
- b) frequently asked questions and information chatbots;

- c) scheduling optimization;
- d) invoice categorization;
- e) library discovery support;
- f) routine analytics; and
- g) workflow assistance.

The following decisions shall require accountable human decision-making:

- a) admission;
- b) scholarship awards;
- c) disciplinary action;
- d) final grades and academic standing;
- e) employment selection and termination;
- f) health or welfare decisions; and
- g) other decisions with comparable impact on rights or significant interests.
- h) AI shall not be used for covert surveillance or behavioural scoring of students or staff without lawful authority, demonstrated necessity, proportionality and approved safeguards.
- i) AI-generated recommendations affecting individuals shall be sufficiently understandable to permit responsible human review.
- j) Persons affected by AI-assisted decisions shall have access to a human route for reconsideration.

5.3 Health, Clinical, Legal, Engineering and Other High-Stakes Uses

1. Where University programmes or services involve health, legal, safety or other regulated decisions, AI shall function as decision support rather than autonomous professional authority unless expressly permitted by the competent regulator.
2. Clinical AI outputs shall receive qualified human review and shall not substitute for professional judgement.
3. Student AI use during clinical or other professional placements shall comply with patient/client confidentiality and applicable professional rules.
4. Legal, clinical, engineering and other regulated outputs shall be checked against authoritative primary sources and current professional standards.
5. AI use shall not introduce an unacceptable risk to patients, clients, research participants, students, staff or the public.

5.4 Equity, Accessibility, Connectivity and Inclusion

1. The University shall not assume that every student has a recent computer, uninterrupted broadband, a paid AI subscription or equal proficiency in academic English.
2. Where AI is required for learning or assessment, the University shall provide scheduled access through University facilities or another approved institutional route.
3. A paid proprietary AI subscription shall not be a hidden course requirement unless the University provides an equitable access route.
4. Where practicable, courses and services shall provide mobile-conscious and low-bandwidth alternatives.
5. Where AI is optional, a non-AI route shall be available where absence of AI would otherwise disadvantage a student.
6. Accessibility features such as captioning, text-to-speech and alternative formats may be used subject to privacy and security controls.
7. AI-supported language access may be encouraged, but AI shall not replace development of students' required communication competence.
8. The University may support research and development involving Hausa, Yoruba, Igbo, Nigerian English and other African languages relevant to its mission, subject to applicable rights, ethical requirements and protection of cultural knowledge.

5.5 Intellectual Property, Copyright and Confidentiality

1. AI output shall not be presumed to be owned by IBBU, a staff member or a student. Ownership and permitted use shall be determined under applicable law, contract and University rules.
2. Copyrighted, licensed, confidential or third-party material shall not be uploaded to an AI system where the applicable licence, law, contract or University rule does not permit such use.
3. AI-generated text, images, code and other outputs used in scholarly or institutional work shall be reviewed for provenance, infringement and applicable disclosure requirements.
4. University-owned confidential information remains subject to University intellectual-property and confidentiality requirements regardless of the device, account or AI platform used.

SECTION SIX: AI MISCONDUCT AND DISCIPLINARY MEASURES

6.1 Academic Integrity and Misconduct

AI-related misconduct shall be addressed under the University's existing academic integrity, disciplinary and research-misconduct procedures. This Policy does not create a separate punishment regime.

Conduct may constitute academic or research misconduct where a person:

1. submits AI-generated work as their own when independent work is required;
2. fails to disclose AI use where disclosure is expressly required;
3. uses AI in an assessment where its use is expressly prohibited;
4. fabricates references, evidence, data, quotations or results through AI;
5. processes data or confidential information using AI without authorisation; or
6. manipulates AI outputs or synthetic media to misrepresent scholarship, identity, evidence or University records.

No finding of misconduct shall be made without notice of the allegation, an opportunity to respond, and consideration under the University's due-process procedures. An AI-detection score alone shall not constitute sufficient evidence of misconduct.

6.2 Prohibited Uses

Unless expressly authorised by Senate and lawful under applicable requirements, the following are prohibited:

1. fully automated high-impact decisions affecting admission, scholarships, progression, discipline, employment, health, safety or comparable significant interests;
2. covert surveillance or behavioural scoring of students or staff without lawful authority, necessity, proportionality and approved safeguards;
3. fabrication or manipulation of research data, results, participants, sources, citations, quotations or other scholarly evidence;
4. unauthorised processing or disclosure of sensitive personal, confidential, restricted or security information through AI;
5. use of an institutional AI system without an identified owner and required approval; and
6. use of AI in a manner that violates applicable law, University rules, professional standards, contractual obligations or approved assessment conditions.

6.3 Penalties and Disciplinary Measures

6.3.1 General Principle

Any person who violates this Policy may be subject to corrective, academic, administrative, disciplinary or other lawful measures in accordance with applicable University regulations. Misconduct shall be judged by whether AI use breached requirements, caused or risked harm, involved deception, or violated University rules.

6.3.2 Factors to be Considered

In determining an appropriate response, the University shall consider:

1. the nature and seriousness of the violation;
2. whether AI use was prohibited, restricted, permitted or required;
3. whether the conduct was intentional, reckless or negligent;
4. whether deception or misrepresentation occurred;
5. the impact on fairness, integrity or reliability of an assessment, research activity or institutional record;
6. whether sensitive or confidential information was improperly disclosed;
7. the actual or potential harm caused;
8. whether an unfair advantage was sought;
9. cooperation with investigation and corrective measures;
10. prior violations; and
11. any other relevant circumstances under University procedures.

6.3.3 Possible Measures

Depending on the case, measures may include:

1. advice, warning or formal caution;
2. mandatory training or remedial instruction;
3. correction, resubmission or repetition of affected work;
4. invalidation of an assessment component or reduction of marks;
5. withdrawal or suspension of access to AI systems or University facilities;
6. requirement to secure or delete improperly submitted information;
7. disciplinary action under student or staff regulations;
8. research-related corrective measures, including correction or withdrawal of outputs;

9. referral to professional, regulatory, legal or security authorities where required; and
10. any other lawful measure authorised under University regulations.

6.3.4 Proportionality

Penalties shall be proportionate to the seriousness and circumstances of the violation. Minor, inadvertent or first-time breaches may attract educational or corrective responses, while deliberate deception, repeated misconduct or serious harm may warrant stronger sanctions.

6.4 Specific Contexts

6.4.1 Academic Assessment

Where AI misuse affects an assessment, consequences shall be determined under the University's academic-integrity and assessment regulations. The presence of AI-generated content alone does not establish misconduct. Instructions, permissions, explanations and evidence shall be considered in full.

6.4.2 Research and Scholarship

Fabrication, manipulation or false representation of research data, results, sources, citations or other scholarly material through AI shall be investigated under research-integrity procedures. Corrective action may extend to affected publications, datasets, collaborators or funders.

6.4.3 Data Protection and Confidentiality

Submitting personal, confidential or restricted information to an AI system without authorisation shall be managed under the University's data-protection and information-security procedures. Immediate containment or deletion may be required, alongside disciplinary or lawful consequences.

6.4.4 Institutional AI Systems

Unauthorised deployment or operation of AI systems without approval, risk assessment, registration, security controls or oversight may result in suspension or restriction of the system. Where negligence or deliberate circumvention is established, disciplinary or contractual measures may apply.

6.5 Due Process and Appeals

No penalty shall be imposed without the affected person being informed of the allegation, given a reasonable opportunity to respond, and entitled to appeal under the University's procedures. Decisions shall be reasoned, recorded and made only by competent authorities.

6.6 Record-Keeping and Policy Learning

Records of AI-related disciplinary and corrective actions shall be maintained in line with University privacy and confidentiality requirements. Aggregated or anonymised information may be used to identify risks, improve training, strengthen assessment design, update controls and inform periodic policy review.

Draft Copy

SECTION SEVEN: AI IMPLEMENTATION, MONITORING AND RESPONSIBILITIES

7.1 Staff Development and Support

1. Academic and relevant professional staff shall receive introductory training on AI governance, academic integrity and responsible AI use.
2. Academic staff shall have access to discipline-specific assessment redesign and AI-literacy development.
3. Administrative staff who process personal information shall receive relevant AI, privacy and data-protection training.
4. ICT staff, librarians, researchers and designated AI Leads shall receive advanced training appropriate to their responsibilities.
5. Students shall receive AI-literacy and academic-integrity orientation.
6. Training shall be competency-based and shall not depend on a particular AI brand or product.

7.2 Approved Tools and AI Register

The University shall maintain an approved-tool and AI Register outside the core Policy. The Register shall be maintained by ICT in consultation with the **Data Protection Officer** and UAIGC and shall be reviewed at least quarterly.

Register field	Required information
System/tool	Name and provider; version where relevant.
Purpose	Approved institutional use case.
Risk level	Level 1, 2, 3 or 4.
Data class	Public, internal, confidential or sensitive.
Owner	Named business and technical owners.
Approval date	Date and approving authority.
Review date	Next review date.
Controls	Privacy, security, human oversight and access controls.
Restrictions	Activities or data that users must not submit or perform.
Exit plan	Data deletion, export and migration arrangements.

7.3 Incident Management

AI-related incidents shall be managed under applicable University incident, security, privacy and disciplinary procedures. At a minimum, the responsible unit shall:

1. stop, suspend or contain the affected AI process where necessary;
2. notify the responsible University unit, ICT/security function and Data Protection Officer where personal data may be involved;
3. preserve relevant logs, prompts, outputs and other evidence subject to privacy requirements;
4. assess harm, affected persons and applicable regulatory or reporting obligations;
5. correct the affected decision, record or process where required; and
6. conduct a post-incident review and update controls, training or guidance where necessary.

7.4 Monitoring, Evaluation and Reporting

The University shall monitor implementation of this Policy using indicators that include:

1. percentage of active courses with explicit AI assessment guidance;
2. percentage of first-year students completing foundational AI literacy;
3. percentage of academic and relevant professional staff completing required training;
4. availability and use of University-provided AI access and reported access barriers;
5. percentage of programmes completing review of major assessments for AI-related vulnerabilities;
6. number and severity of AI-related privacy and security incidents;
7. percentage of institutional AI systems recorded in the AI Register;
8. AI-related academic integrity and research-misconduct cases and their outcomes;
9. number and outcomes of controlled AI pilots; and
10. annual student and staff feedback on clarity, fairness, transparency and usefulness of AI governance.

The UAIGC shall submit an annual AI governance and implementation report to Senate. The report shall identify significant risks, incidents, implementation gaps, corrective actions, emerging issues and recommended policy or operational changes.

24. Roles and Responsibilities

Actor	Core responsibility
Senate	Approve this Policy; receive annual reports; approve major amendments and any Level 4 exception expressly reserved to Senate.
Vice-Chancellor/Management	Provide institutional leadership, resources and accountability for implementation.
DVC (Academic)	Chair of UAIGC; coordinate academic implementation.
Coordinating Director of Research	Coordinate research governance and responsible innovation.

Registrar	Coordinate administrative governance and institutional records.
ICT Directorate	Technical security, system evaluation, access control, approved-tool administration and AI Register maintenance.
Data Protection Officer	Privacy, data-protection review and compliance.
Library/Information Services	AI literacy, research support, information verification and scholarly communication.
Quality Assurance	Programme-level integration, assessment quality and monitoring.
Faculty/College AI Leads	Discipline-specific implementation, guidance, staff support and escalation.
Academic staff	Set clear course rules; design valid assessments; exercise human judgement; and use AI responsibly.
Researchers	Protect research integrity and data; document material AI use; and comply with ethics and disclosure requirements.
Students	Follow course and assessment rules; disclose material AI use where required; verify outputs; and retain responsibility for submitted work.
Vendors/Contractors	Comply with University contractual, privacy, security, audit and data-handling requirements.

SECTION EIGHT: COMMENCEMENT, REVIEW AND AMENDMENT

8.1. Policy Review and Amendment

The UAIGC shall conduct an annual policy effectiveness and implementation review and shall submit the outcome to Senate.

This Policy shall undergo a formal review at least once every two years and earlier where required by a material change in law, regulation, institutional risk, AI capability or evidence.

Operational guidance, approved-tool lists, templates and technical controls may be amended by the competent University authority under delegated authority without reopening the entire Policy, provided that such amendments do not conflict with this Policy or exceed the authority delegated to the approving body.

Any amendment to the substantive provisions of this Policy shall require approval through the University's established policy approval process, including Senate approval where required.

8.2 Effective Date and Transitional Provision

This Policy shall take effect on 1 January 2027.

Within three months of the effective date, the University shall establish the UAIGC and commence an audit of existing institutional AI use. Within six months, the University shall establish the AI Register, approve the risk-governance process and commence foundational staff and student training. Faculties and Colleges shall thereafter implement assessment-level AI statements and review priority assessments in accordance with this Policy.

Existing institutional AI systems shall be reviewed and entered into the AI Register within twelve months of the effective date. Systems that do not satisfy the requirements of this Policy shall be suspended, remediated or retired in accordance with the University's governance and procurement procedures.

APPENDIX

Appendix A: Model Course AI Statement

Artificial Intelligence and Academic Integrity: AI use in this course is governed at the assessment level. For each assessment, the instructions will state whether AI is prohibited, permitted for specified assistance, permitted as a collaborative tool, or required as part of the learning outcome. Where AI use is permitted or required, students must comply with the stated disclosure requirements and remain responsible for the accuracy, citations, reasoning and final work submitted. When uncertain, ask the course lecturer before using AI.

Appendix B: Student AI Disclosure Statement

(Complete if AI was used)

COURSE: [Course Code & Title]

ASSIGNMENT: [Assignment Name]

DATE SUBMITTED: [Date]

I used the following AI tool(s) on this assignment:

Tool Name & Version:

Purpose(s) (check all that apply):

- ☐ Brainstorming / Ideation
- ☐ Organizing / Outlining structure
- ☐ Drafting / Generating text
- ☐ Proofreading / Grammar correction
- ☐ Data analysis / Processing
- ☐ Language translation
- ☐ Other: _____

Specific Contribution (describe what the AI generated and what you revised/added):

[Your explanation here]

I have verified all AI-generated content for:

- ☐ Factual accuracy
- ☐ Proper citations & references
- ☐ Alignment with the assignment requirements

This final work represents my own analysis, understanding, and voice.

Signed: _____

Date: _____