

MCPHERSON UNIVERSITY

SERIKI-SOTAYO, OGUN STATE, NIGERIA

“To Build a People of Excellence and Integrity for Service”



ARTIFICIAL INTELLIGENCE POLICY

Comprehensive Institutional Governance Framework for Teaching, Learning, Research, Data Protection, and Operations

Promulgating Authority

Senate of McPherson University

Document Reference Code

McU/SEN/POL/2026/AI-01

Effective Date & Version

September 2026 | Version 1.0 (Official Press Edition)

Statutory Alignment

NUC AI Policy Framework, NDPA 2023, NAIS 2025–2029

Document Custodian

Office of the Vice-Chancellor & ICT Directorate

TABLE OF CONTENTS

PART ONE: FOUNDATIONAL PROVISIONS	11
SECTION 1: PREAMBLE AND INSTITUTIONAL CONTEXT	11
1.1 <i>McPherson University: Identity and Foundation</i>	11
1.2 <i>Vision and Mission</i>	11
1.3 <i>The Emergence of Artificial Intelligence in Higher Education</i>	11
1.4 <i>Governance Gap and Institutional Response</i>	11
1.5 <i>The University's Digitalisation Trajectory</i>	12
1.6 <i>Senate Authority and Policy Status</i>	12
SECTION 2: PURPOSE OF THE POLICY	12
2.1 <i>Primary Purposes</i>	12
2.2 <i>Distinctive Institutional Purposes</i>	13
SECTION 3: SCOPE AND APPLICATION	13
3.1 <i>Persons Covered</i>	13
3.2 <i>Activities Covered</i>	13
3.3 <i>Devices and Platforms Covered</i>	14
3.4 <i>Relationship to Existing Policies</i>	14
3.5 <i>Exclusions</i>	14
SECTION 4: DEFINITIONS AND INTERPRETATION.....	15
4.1 <i>Artificial Intelligence (AI)</i>	15
4.2 <i>Generative AI</i>	15
4.3 <i>Large Language Model (LLM)</i>	15
4.4 <i>Machine Learning</i>	15
4.5 <i>Automated Decision-Making</i>	15
4.6 <i>AI-Assisted Work</i>	15
4.7 <i>AI-Generated Content</i>	15
4.8 <i>Prompt</i>	16
4.9 <i>Training Data</i>	16
4.10 <i>Algorithmic Bias</i>	16
4.11 <i>Human Oversight</i>	16
4.12 <i>Explainability and Interpretability</i>	16
4.13 <i>Data Controller and Data Subject</i>	16
4.14 <i>Personal Data and Sensitive Personal Data</i>	16
4.15 <i>Other Operative Terms</i>	16
4.16 <i>Rules of Interpretation</i>	17
PART TWO: GOVERNING PRINCIPLES	18
SECTION 5: CORE PRINCIPLES FOR AI AT MCPHERSON UNIVERSITY	18
5.1 <i>Human-Centred Governance</i>	18
5.2 <i>Academic Integrity</i>	18
5.3 <i>Transparency and Disclosure</i>	18
5.4 <i>Accountability</i>	19
5.5 <i>Equity and Inclusion</i>	19
5.6 <i>Privacy and Data Protection</i>	19
5.7 <i>Security and Reliability</i>	19

5.8 Stewardship of Institutional Values.....	20
5.9 Continuous Learning.....	20
5.10 Proportionality.....	20
SECTION 6: ALIGNMENT WITH NATIONAL REGULATORY FRAMEWORK.....	20
6.1 The NUC Artificial Intelligence Policy Framework.....	20
6.2 Integration of AI Competencies Under CCMAS.....	21
6.3 The Nigeria National Artificial Intelligence Strategy 2025–2029.....	21
6.4 The Nigeria Data Protection Act 2023.....	22
6.5 The Nigeria Data Protection Act General Application and Implementation Directive 2025.....	22
6.6 The Cybercrimes (Amendment) Act 2024.....	22
6.7 The Nigerian Ethical AI Framework.....	23
6.8 NUC Compliance Monitoring and Reporting.....	23
SECTION 7: ALIGNMENT WITH INTERNATIONAL BEST PRACTICE.....	23
7.1 UNESCO Recommendation on the Ethics of Artificial Intelligence.....	23
7.2 OECD AI Principles.....	24
7.3 Comparative Approaches from Leading University AI Policies.....	24
7.4 McPherson University's Distinctive Contribution.....	24
PART THREE: AI IN TEACHING, LEARNING, AND ASSESSMENT	25
SECTION 8: AI AND ACADEMIC INTEGRITY.....	25
8.1 Foundational Position.....	25
8.2 Definition of Academic Misconduct in the AI Context.....	25
8.3 Permitted Uses of AI in Academic Work.....	25
8.4 Disclosure Requirements.....	26
8.5 Course-Level AI Guidelines.....	26
8.6 Detection and Investigation of AI-Related Misconduct.....	27
8.7 Penalties and Remediation.....	27
8.8 Appeals and Due Process.....	27
8.9 Staff Academic Integrity Obligations.....	28
SECTION 9: COURSE-LEVEL AI GUIDELINES.....	28
9.1 Faculty Responsibility.....	28
9.2 The Five-Category AI Use Scale.....	28
9.3 Syllabus Statements on AI Use.....	29
9.4 Assignment-Level AI Use Mapping.....	29
9.5 Disclosure Requirements for AI-Assisted Work.....	29
9.6 Citation and Attribution Standards for AI-Generated Content.....	30
9.7 Verification and Fact-Checking Requirements.....	30
9.8 Accommodations for Students with Disabilities.....	30
9.9 Equity Considerations in AI-Enabled Assessment.....	30
SECTION 10: AI LITERACY AND STUDENT DEVELOPMENT.....	31
10.1 Embedding AI Literacy Across All Programmes.....	31
10.2 University-Wide AI Literacy Requirement.....	31
10.3 Critical Evaluation of AI Outputs.....	31
10.4 Ethical Reasoning About AI.....	31
10.5 Prompt Engineering and Effective AI Collaboration.....	32
10.6 Understanding Algorithmic Bias and Limitations.....	32
10.7 Preparing Graduates for AI-Augmented Workplaces.....	32

10.8 Co-Curricular AI Learning Opportunities	32
SECTION 11: FACULTY AND TEACHING STAFF RESPONSIBILITIES	33
11.1 Designing AI-Resilient Assessments	33
11.2 Modelling Responsible AI Use	33
11.3 Providing Clear Guidance to Students	33
11.4 Ongoing Professional Development in AI Pedagogy	34
11.5 Reporting AI-Related Concerns	34
11.6 Balancing Innovation with Integrity	34
PART FOUR: AI IN RESEARCH AND SCHOLARSHIP	35
SECTION 12: AI IN RESEARCH	35
12.1 Foundational Position	35
12.2 Permitted Uses of AI in Research	35
12.3 Prohibited Uses of AI in Research	36
12.4 Disclosure and Attribution of AI Contributions to Research	36
12.5 AI in Literature Review and Systematic Synthesis	37
12.6 AI in Data Collection and Processing	37
12.7 AI in Experimental Design and Simulation	37
12.8 Compliance with Funder and Journal Requirements	38
12.9 Intellectual Property Considerations	38
SECTION 13: RESEARCH ETHICS AND AI	38
13.1 Ethical Review Requirements for AI-Related Research	38
13.2 Protection of Human Subjects in AI Research	38
13.3 Avoidance of Algorithmic Harm	39
13.4 Data Sovereignty and Local Relevance	39
13.5 Research on Africa-Priority Themes Using AI	39
13.6 Collaborations with External AI Research Partners	40
13.7 Commercialisation and Technology Transfer	40
SECTION 14: POSTGRADUATE RESEARCH AND AI	40
14.1 AI Use in Thesis and Dissertation Work	40
14.2 Supervisor Responsibilities	41
14.3 Examination and Viva Voce Considerations	41
14.4 Research Integrity Training for Postgraduate Students	42
14.5 AI in Postgraduate Coursework	42
PART FIVE: AI IN ADMINISTRATION AND OPERATIONS	43
SECTION 15: ADMINISTRATIVE USE OF AI	43
15.1 Foundational Position	43
15.2 Permitted Administrative Applications	43
15.3 Prohibited Administrative Applications	44
15.4 Human Oversight Requirements for AI-Assisted Administrative Decisions	44
15.5 Procurement and Evaluation of AI Tools	45
15.6 Vendor and Third-Party AI Service Agreements	45
15.7 Integration with Existing University Systems	46
15.8 Training for Administrative Staff	46
SECTION 16: STUDENT RECORDS, ADMISSIONS, AND ASSESSMENT ADMINISTRATION	47
16.1 AI in Admissions Processes	47

16.2 AI in Student Records Management	47
16.3 AI in Academic Advising	47
16.4 AI in Examination Administration.....	48
16.5 Automated Decision-Making Restrictions Under NDPA	48
16.6 Right to Human Review of Automated Decisions.....	49
16.7 Data Retention and Disposal	49
SECTION 17: FINANCE, PROCUREMENT, AND RESOURCE MANAGEMENT	49
17.1 AI in Budgeting and Financial Planning	49
17.2 AI in Procurement and Vendor Management.....	50
17.3 Cost-Benefit Assessment for AI Investments	50
17.4 Licensing and Subscription Management	50
17.5 Sustainability Considerations	50
SECTION 18: HUMAN RESOURCES AND STAFF MANAGEMENT	51
18.1 AI in Recruitment and Selection.....	51
18.2 AI in Performance Management	51
18.3 AI in Staff Development and Training.....	52
18.4 Protection of Staff Data.....	52
18.5 AI-Related Job Displacement and Reskilling.....	52
18.6 Staff Rights in AI-Augmented Workplaces	52
PART SIX: DATA GOVERNANCE AND PRIVACY.....	54
SECTION 19: DATA PROTECTION FRAMEWORK.....	54
19.1 Foundational Position.....	54
19.2 Compliance with the Nigeria Data Protection Act 2023.....	54
19.3 Lawful Bases for Processing Personal Data.....	54
19.4 Data Protection Officer Designation and Responsibilities	55
19.5 Data Privacy Impact Assessments for AI Systems.....	56
19.6 Consent Requirements for AI Processing.....	56
19.7 Data Subject Rights	57
19.8 Automated Decision-Making Restrictions Under NDPA Section 37	57
19.9 Cross-Border Data Transfer Rules	58
19.10 Data Breach Notification and Response	58
SECTION 20: INSTITUTIONAL DATA GOVERNANCE FOR AI.....	59
20.1 Data Governance Framework.....	59
20.2 Classification of University Data	59
20.3 Ownership and Stewardship of Institutional Data	59
20.4 Data Quality Standards for AI Training and Operation.....	60
20.5 Prohibition on Using Institutional Data for Unauthorised AI Training	60
20.6 Data Minimisation and Purpose Limitation.....	60
20.7 Audit Trails and Logging for AI Systems	61
20.8 Data Retention and Disposal Schedules	61
SECTION 21: PRIVACY OF STUDENT AND STAFF DATA	61
21.1 Protection of Student Academic Records	61
21.2 Protection of Staff Personnel Records	62
21.3 Protection of Health and Counselling Data.....	62
21.4 Protection of Research Participant Data.....	62
21.5 Prohibition on Unauthorised AI Profiling	63

21.6 Transparency Regarding AI Processing of Personal Data.....	63
PART SEVEN: INFRASTRUCTURE, SECURITY, AND RISK MANAGEMENT.....	64
SECTION 22: ICT INFRASTRUCTURE AND AI READINESS.....	64
22.1 Foundational Position.....	64
22.2 Assessment of Current ICT Capacity for AI.....	64
22.3 Internet Connectivity and Bandwidth Requirements.....	64
22.4 Computing Resources for AI Research and Teaching.....	65
22.5 Cloud Services and Storage.....	65
22.6 Power Reliability and Business Continuity.....	66
22.7 Accessibility of AI Tools for All Students and Staff.....	66
22.8 Infrastructure Development Roadmap.....	66
SECTION 23: CYBERSECURITY AND AI.....	67
23.1 Foundational Position.....	67
23.2 AI-Related Cybersecurity Risks.....	67
23.3 Protection of AI Systems from Unauthorised Access.....	67
23.4 Secure Development and Deployment Practices.....	68
23.5 Incident Response for AI-Related Security Breaches.....	68
23.6 Compliance with the Cybercrimes (Amendment) Act 2024.....	69
23.7 Prohibition on Malicious AI Use.....	69
23.8 Staff and Student Cybersecurity Awareness.....	69
SECTION 24: RISK MANAGEMENT FRAMEWORK.....	70
24.1 Foundational Position.....	70
24.2 AI Risk Identification and Assessment.....	70
24.3 Risk Categorisation.....	70
24.4 Risk Mitigation Strategies.....	71
24.5 AI System Registration and Inventory.....	71
24.6 Regular Risk Reviews and Audits.....	72
24.7 Insurance and Liability Considerations.....	72
24.8 Business Continuity and Disaster Recovery for AI Systems.....	72
SECTION 25: THIRD-PARTY AI TOOLS AND SERVICES.....	73
25.1 Foundational Position.....	73
25.2 Approved AI Tools and Platforms.....	73
25.3 Evaluation Criteria for Third-Party AI Services.....	73
25.4 Data Processing Agreements with Vendors.....	74
25.5 Vendor Security and Privacy Assessments.....	74
25.6 Prohibition on Unauthorised AI Tool Use.....	75
25.7 Monitoring and Review of Third-Party AI Services.....	75
25.8 Exit Strategies and Data Portability.....	76
PART EIGHT: CAPACITY BUILDING AND CULTURE.....	77
SECTION 26: AI LITERACY AND TRAINING.....	77
26.1 Foundational Position.....	77
26.2 Baseline AI Literacy for All Students.....	77
26.3 AI Competency Framework for Staff.....	78
26.4 Role-Specific Training.....	78
26.5 Continuing Professional Development in AI.....	79

26.6 Certification and Recognition of AI Competencies	79
26.7 Training Resources and Delivery Mechanisms	80
SECTION 27: AWARENESS AND COMMUNICATION	80
27.1 Foundational Position	80
27.2 Communicating the Policy to the University Community	80
27.3 Regular Updates on AI Developments	81
27.4 Sharing of Best Practices	81
27.5 Student and Staff Engagement Mechanisms	81
27.6 External Communication and Public Engagement	82
27.7 Integration with University Website and NUC Ranking Requirements	82
SECTION 28: RESEARCH AND INNOVATION PROMOTION	82
28.1 Foundational Position	82
28.2 Encouraging AI-Related Research	83
28.3 Interdisciplinary AI Research Initiatives	83
28.4 Collaboration with Industry and Other Institutions	84
28.5 AI Innovation and Entrepreneurship	84
28.6 Funding and Resource Support for AI Research	84
28.7 Dissemination and Knowledge Sharing	85
PART NINE: GOVERNANCE AND ACCOUNTABILITY	86
SECTION 29: GOVERNANCE STRUCTURE	86
29.1 Foundational Position	86
29.2 University Senate	86
29.3 AI Policy Committee	87
29.4 College AI Representatives	88
29.5 ICT Directorate	88
29.6 Data Protection Officer	89
29.7 Research Ethics Committee	89
29.8 Library and Information Services	90
29.9 Student Affairs	90
29.10 Governing Council	90
29.11 External Advisory Engagement	91
SECTION 30: ROLES AND RESPONSIBILITIES	91
30.1 Purpose of This Section	91
30.2 Senate	91
30.3 Vice-Chancellor and Management	91
30.4 AI Policy Committee	92
30.5 Deans and Heads of Department	92
30.6 Academic Staff	92
30.7 Administrative Staff	93
30.8 Students	93
30.9 ICT Staff	93
30.10 Data Protection Officer	94
30.11 Library Staff	94
30.12 External Partners and Vendors	94
SECTION 31: COMPLIANCE AND MONITORING	94
31.1 Foundational Position	94

31.2 Compliance Requirements for All University Members.....	95
31.3 Regular Monitoring of AI Use.....	95
31.4 Annual AI Policy Compliance Report to Senate	95
31.5 Internal Audits of AI Systems and Practices	96
31.6 NUC Compliance Monitoring Preparation.....	96
31.7 Corrective Action for Non-Compliance	97
31.8 Whistleblower Protections	97
SECTION 32: REVIEW AND AMENDMENT.....	97
32.1 Foundational Position.....	97
32.2 Scheduled Policy Review.....	97
32.3 Triggers for Unscheduled Review.....	98
32.4 Amendment Procedure	98
32.5 Version Control and Documentation	98
32.6 Stakeholder Consultation in Review.....	99
32.7 Alignment with National Review Cycles	99
PART TEN: IMPLEMENTATION AND TRANSITION	100
SECTION 33: IMPLEMENTATION PLAN	100
33.1 Foundational Position.....	100
33.2 Phased Implementation Timeline.....	100
33.3 Immediate Priorities.....	103
33.4 Resource Requirements and Budget.....	103
33.5 Risk Mitigation During Transition.....	104
SECTION 34: RESOURCE MOBILISATION.....	104
34.1 Foundational Position.....	104
34.2 Budget Allocation for AI Infrastructure and Training	104
34.3 Internal Resource Reallocation.....	105
34.4 External Funding Opportunities	105
34.5 Industry Collaboration and Sponsorship	106
34.6 Cost-Sharing Mechanisms.....	106
34.7 Sustainability Planning	107
SECTION 35: STAKEHOLDER ENGAGEMENT	107
35.1 Foundational Position.....	107
35.2 Senate and Management Consultation.....	107
35.3 Faculty and Staff Consultation.....	108
35.4 Student Consultation	108
35.5 Alumni and Community Engagement.....	109
35.6 Industry and Professional Body Engagement	109
35.7 Regulatory Agency Engagement	109
35.8 International Partner Engagement	109
35.9 Engagement Mechanisms and Feedback Loops.....	110
SECTION 36: POLICY LAUNCH AND COMMUNICATION.....	110
36.1 Foundational Position.....	110
36.2 Official Launch and Dissemination.....	110
36.3 Website Publication and Accessibility	111
36.4 Orientation Sessions.....	111
36.5 Integration with Student and Staff Handbooks.....	111

36.6 NUC Notification and Ranking Documentation.....	112
36.7 Communication Strategy Principles.....	112
36.8 First-Year Communication Priorities	112
36.9 Measuring Communication Effectiveness	113
PART ELEVEN: MISCELLANEOUS AND SUPPLEMENTARY PROVISIONS.....	114
SECTION 37: RELATIONSHIP TO OTHER UNIVERSITY POLICIES.....	114
37.1 Foundational Position.....	114
37.2 Academic Integrity Policy	114
37.3 ICT Acceptable Use Policy	114
37.4 Research Ethics Policy.....	115
37.5 Data Protection Policy.....	115
37.6 Human Resources Policy	116
37.7 Student Handbook	116
37.8 Staff Handbook.....	116
37.9 Conflict Resolution Between Policies.....	117
SECTION 38: LEGAL COMPLIANCE AND LIABILITY	117
38.1 Foundational Position.....	117
38.2 Compliance with Nigerian Law.....	117
38.3 Liability for AI-Related Harm	118
38.4 Indemnification and Insurance.....	118
38.5 Dispute Resolution	118
38.6 Governing Law.....	119
SECTION 39: SPECIAL PROVISIONS FOR SPECIFIC PROGRAMMES.....	119
39.1 Foundational Position.....	119
39.2 College of Computing.....	119
39.3 College of Allied Health Sciences	119
39.4 College of Law	120
39.5 College of Natural and Applied Sciences.....	120
39.6 College of Humanities, Social and Management Sciences	120
39.7 Postgraduate Studies.....	121
39.8 JUPEB Foundation School	121
SECTION 40: TRANSITIONAL ARRANGEMENTS.....	121
40.1 Effective Date of the Policy.....	121
40.2 Grace Period for Compliance.....	122
40.3 Grandfathering of Existing AI Tools and Practices	122
40.4 Interim Governance Arrangements	122
40.5 First Review Timeline.....	123
SECTION 41: INTERPRETATION AND DEFINITIONS (CONSOLIDATED).....	123
41.1 Full Glossary of Terms.....	123
41.2 Rules of Interpretation	124
41.3 Severability.....	124
41.4 Waiver	124
SECTION 42: APPENDICES	125
Appendix A: AI Use Categories (Five-Level Scale)	125
Appendix B: AI Use Disclosure Form.....	128
Appendix C: Reflective AI Use Statement Template.....	130

<i>Appendix D: Privacy and Responsible Use Checklist.....</i>	<i>132</i>
<i>Appendix E: AI Tool Evaluation Criteria.....</i>	<i>133</i>
<i>Appendix F: Data Privacy Impact Assessment Template.....</i>	<i>136</i>
<i>Appendix G: AI Incident Reporting Form.....</i>	<i>138</i>
<i>Appendix H: NUC AI Policy Framework Alignment Matrix.....</i>	<i>140</i>
<i>Appendix I: NAIS Pillar Alignment Matrix.....</i>	<i>141</i>
<i>Appendix J: Glossary of Technical Terms</i>	<i>142</i>
<i>Appendix K: Reference List.....</i>	<i>144</i>

Part One: Foundational Provisions

Section 1: Preamble and Institutional Context

1.1 McPherson University: Identity and Foundation

McPherson University (McU) was licensed by the National Universities Commission on 28 February 2012 as the 49th private university and the 121st university in Nigeria. Founded by the Foursquare Gospel Church in Nigeria and named after Aimee Semple McPherson, the University was established to complement the Church's educational mission and to produce highly skilled human resources for national development.

The University is located at Seriki-Sotayo, Ogun State, on a 302.210-acre campus, and currently serves approximately 5,000 students across five Colleges: Allied Health Sciences, Computing, Law, Humanities, Social and Management Sciences, and Natural and Applied Sciences. The University also operates a College of Postgraduate Studies offering PGD, M.Sc., MPhil, and Ph.D. programmes, and a JUPEB Foundation School for direct entry preparation.

1.2 Vision and Mission

McPherson University's vision is **"To build a people of excellence and integrity for service"**. Its mission is **"To provide qualitative, functional, and sound education with Godly virtues that will prepare men and women for leadership and positive impact on society"**.

These foundational statements are not ceremonial. They constitute the University's binding commitments to quality, character, and social contribution. Any institutional policy, including this Artificial Intelligence Policy, must be assessed against these commitments. The University does not adopt technology for its own sake. It adopts technology that serves its mission of forming people of excellence, integrity, and service.

1.3 The Emergence of Artificial Intelligence in Higher Education

Artificial Intelligence has transitioned from an experimental technology to a strategic capability that is transforming teaching, learning, research methodologies, institutional governance, quality assurance, student services, and university administration across the globe. The central question confronting university administrators is no longer whether AI should be adopted, but how it must be governed, regulated, and deployed responsibly.

For McPherson University, this global transformation presents both an opportunity and an obligation. The opportunity lies in AI's capacity to enhance learning outcomes, accelerate research, streamline administration, and extend the University's reach and impact. The obligation lies in ensuring that AI adoption is consistent with the University's values, protective of its community, compliant with Nigerian law, and aligned with national regulatory expectations.

1.4 Governance Gap and Institutional Response

In July 2026, the National Association of Artificial Intelligence Practitioners (NAAIP), in collaboration with the National Universities Commission (NUC), the National Board for Technical Education (NBTE), and the National Commission for Colleges of Education (NCCE), convened its fifth national symposium on AI governance in Nigerian higher education. The symposium officially signaled an end to the era of ad-hoc, isolated AI guidelines in tertiary institutions and affirmed the need for unified regulatory guardrails.

The NUC has developed the landmark Artificial Intelligence Policy Framework and Implementation Roadmap for the Nigerian University System, providing a structured framework for responsible AI integration. The NUC has also committed to enforcing compliance through two mandatory mechanisms: rigorous, periodic monitoring of individual university AI development using a standardized reporting template, and structured programmes for enhanced human capacity development on AI across the Nigerian University System.

McPherson University adopts this policy in response to these national developments and in recognition of its own institutional responsibilities. This policy positions the University as a responsible adopter and contributor to Nigeria's emerging AI governance framework, rather than a passive recipient of external directives.

1.5 The University's Digitalisation Trajectory

McPherson University has been steadily strengthening its digital infrastructure and administrative systems. The University is equipped with modern ICT facilities and has been investing in library automation, e-resource access, and administrative digitalisation. Recent capacity-building initiatives have focused on modernising library services and enhancing staff digital competencies. The University has also been expanding its academic programmes in computing and related fields, with the recent addition of Data Science to its approved programme portfolio.

This policy builds upon that trajectory. It is not a stand-alone intervention but an integration of AI governance into the University's broader digitalisation and quality-improvement strategy.

1.6 Senate Authority and Policy Status

This policy is issued under the authority of the Senate of McPherson University as the principal academic governance body responsible for academic standards, curriculum, research direction, and institutional quality assurance. Upon approval, this policy shall be binding on all members of the University community. It shall be subject to periodic review as provided in Section 32.

Section 2: Purpose of the Policy

2.1 Primary Purposes

The purposes of this policy are:

- (a) **To establish a unified institutional framework for the responsible use of Artificial Intelligence** across all Colleges, programmes, and administrative units of McPherson University.
- (b) **To protect academic integrity** while enabling legitimate, pedagogically sound AI-assisted learning and assessment.
- (c) **To ensure compliance** with Nigerian law, NUC regulatory guidance, and applicable international standards.
- (d) **To position McPherson University as a leader** among Nigerian private universities in ethical AI adoption and governance.

(e) **To provide clarity, consistency, and accountability** in all AI-related decisions, practices, and investments.

(f) **To support the University's mission** by ensuring that AI adoption serves the formation of people of excellence, integrity, and service.

2.2 Distinctive Institutional Purposes

In addition to the general purposes above, this policy serves three distinctive purposes that arise from McPherson University's particular identity:

First, to ensure that AI use is consistent with the University's Christian ethical foundations. McPherson University was founded by the Foursquare Gospel Church and maintains a commitment to Godly virtues as expressed in its mission statement. This policy translates that commitment into concrete AI governance principles, addressing questions of honesty, stewardship, human dignity, and the common good.

Second, to prepare graduates for AI-augmented professional environments. As AI becomes embedded in healthcare, law, business, education, journalism, and public administration, McPherson University graduates must be equipped not merely to use AI tools, but to evaluate them critically, deploy them ethically, and lead in their responsible implementation.

Third, to contribute to Nigeria's national AI development agenda. The Nigeria National Artificial Intelligence Strategy 2025–2029 sets ambitious targets, including equipping at least 70% of Nigeria's young workforce aged 16–35, including 50% women, with AI-related skills. McPherson University, through this policy, commits to contributing to that national objective within its sphere of influence.

Section 3: Scope and Application

3.1 Persons Covered

This policy applies to:

- (a) All **students** enrolled in undergraduate, postgraduate, part-time, JUPEB, and any other programmes of the University, whether on campus or at any other location.
- (b) All **academic staff**, including full-time, part-time, adjunct, visiting, and contract academic personnel.
- (c) All **non-academic staff**, including administrative, technical, library, ICT, works, security, and support personnel.
- (d) All **management personnel**, including the Vice-Chancellor, Deputy Vice-Chancellors, Registrar, Bursar, University Librarian, Deans, Directors, and Heads of Department.
- (e) All **external persons** who use University AI systems, facilities, or data, including visiting researchers, consultants, contractors, and vendors, to the extent specified in their respective agreements with the University.

3.2 Activities Covered

This policy applies to all University-related activities involving AI, including but not limited to:

- (a) **Teaching and learning** — course delivery, assessment, feedback, tutoring, and learning support.
- (b) **Research and scholarship** — research design, data analysis, literature review, writing, publication, and knowledge dissemination.
- (c) **Administration and operations** — admissions, records management, scheduling, finance, procurement, human resources, and correspondence.
- (d) **Student services** — advising, counselling, career services, and co-curricular activities.
- (e) **Governance and quality assurance** — accreditation preparation, compliance monitoring, strategic planning, and institutional reporting.
- (f) **External engagement** — partnerships, industry collaboration, community service, and public communication.

3.3 Devices and Platforms Covered

This policy applies to AI use on:

- (a) University-owned devices, networks, and systems.
- (b) Personally owned devices when used for University business, research, or academic work.
- (c) Third-party AI platforms and services accessed by University community members for University-related purposes, whether or not the University has a formal agreement with the provider.

3.4 Relationship to Existing Policies

This policy shall be read in conjunction with, and does not replace, the following existing or forthcoming University policies:

- (a) Academic Integrity Policy
- (b) ICT Acceptable Use Policy
- (c) Research Ethics Policy
- (d) Data Protection and Privacy Policy
- (e) Staff Handbook
- (f) Student Handbook
- (g) Examination Regulations

Where a conflict arises between this policy and another University policy, the more specific AI-related provision in this policy shall prevail in matters concerning AI, unless the Senate determines otherwise.

3.5 Exclusions

This policy does not apply to:

- (a) AI use by individual community members for purely personal, non-University purposes on personal devices, except where such use directly affects the University's reputation, legal obligations, or the rights of other community members.

(b) AI research conducted under a separate, approved research protocol that has received ethical clearance from the University Research Ethics Committee, where the protocol explicitly addresses AI governance matters in a manner approved by the Committee.

(c) AI systems embedded in third-party tools that are not within the University's control or procurement scope, except to the extent that University data is processed by such tools.

Section 4: Definitions and Interpretation

4.1 Artificial Intelligence (AI)

For the purposes of this policy, **Artificial Intelligence** means the simulation of human intelligence processes by computer systems, including but not limited to systems that perform tasks requiring human-like cognition such as learning, reasoning, problem-solving, perception, language understanding, and decision-making. This includes machine learning, deep learning, natural language processing, computer vision, robotics, expert systems, and generative AI systems.

4.2 Generative AI

Generative AI means AI systems capable of generating new content — including text, images, audio, video, code, and other outputs — in response to prompts or inputs. Examples include large language models (LLMs), text-to-image generators, and code-generation tools.

4.3 Large Language Model (LLM)

Large Language Model means a type of generative AI system trained on vast quantities of text data to understand and generate human-like language. LLMs can produce essays, summaries, translations, code, and conversational responses.

4.4 Machine Learning

Machine Learning means a subset of AI in which systems learn patterns from data and improve their performance on specific tasks without being explicitly programmed for each task.

4.5 Automated Decision-Making

Automated Decision-Making means the process of making decisions about individuals using AI or algorithmic systems without meaningful human involvement. Under the Nigeria Data Protection Act 2023, data subjects have specific rights in relation to automated decision-making, as detailed in Section 19 of this policy.

4.6 AI-Assisted Work

AI-Assisted Work means academic, research, or administrative output that has been produced with some contribution from AI tools, where the human author or decision-maker retains primary creative, analytical, or decision-making responsibility.

4.7 AI-Generated Content

AI-Generated Content means output produced substantially or entirely by an AI system, with limited or no human creative or analytical contribution. The distinction between AI-assisted and AI-generated content is central to this policy's approach to academic integrity.

4.8 Prompt

Prompt means the input, instruction, or query provided by a human user to an AI system to elicit a response or output.

4.9 Training Data

Training Data means the data used to develop, train, or fine-tune an AI model. Training data may include text, images, code, or other information.

4.10 Algorithmic Bias

Algorithmic Bias means systematic and unfair discrimination in AI outputs arising from biased training data, flawed model design, or biased deployment contexts.

4.11 Human Oversight

Human Oversight means the meaningful involvement of a human being in reviewing, approving, or overriding AI-generated recommendations, decisions, or outputs.

4.12 Explainability and Interpretability

Explainability means the extent to which the behaviour and outputs of an AI system can be understood by humans. **Interpretability** means the extent to which the internal logic of an AI model can be understood. Both are relevant to the University's ability to audit and govern AI systems.

4.13 Data Controller and Data Subject

These terms have the meanings assigned to them under the Nigeria Data Protection Act 2023. A **Data Controller** is a person or organisation that determines the purposes and means of processing personal data. A **Data Subject** is an individual whose personal data is processed.

4.14 Personal Data and Sensitive Personal Data

Personal Data means any information relating to an identified or identifiable natural person. **Sensitive Personal Data** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health status, sexual orientation, or biometric data, as defined under the NDPA.

4.15 Other Operative Terms

- (a) **University** means McPherson University.
- (b) **Senate** means the Senate of McPherson University.
- (c) **AI Policy Committee** means the committee established under Section 29.3 of this policy.
- (d) **DPO** means the Data Protection Officer designated by the University under the NDPA.
- (e) **NUC** means the National Universities Commission.
- (f) **NDPA** means the Nigeria Data Protection Act 2023.
- (g) **NAIS** means the Nigeria National Artificial Intelligence Strategy 2025–2029.
- (h) **CCMAS** means the Core Curriculum and Minimum Academic Standards issued by the NUC.

4.16 Rules of Interpretation

- (a) Words importing the singular include the plural and vice versa.
- (b) Headings are for convenience only and do not affect interpretation.
- (c) References to legislation include any amendment or replacement of that legislation.
- (d) References to "Sections" are to Sections of this policy unless otherwise stated.
- (e) Where this policy refers to external standards or frameworks, those references are to the versions current at the date of this policy's approval, and to any subsequent versions adopted by the Senate.

Part Two: Governing Principles

Section 5: Core Principles for AI at McPherson University

The following ten principles constitute the ethical and operational foundation upon which all AI-related decisions, practices, and policies at McPherson University shall be built. These principles are not merely aspirational statements. They are binding interpretive guides for the application of this policy, and they shall be used by the AI Policy Committee, the Senate, and all members of the University community in evaluating AI-related conduct and investments.

5.1 Human-Centred Governance

AI at McPherson University shall serve human flourishing. The University affirms that human beings possess intrinsic dignity that no machine can replicate or replace. AI systems shall be deployed to augment human capabilities, not to substitute for human judgment, moral reasoning, or pastoral care. In all AI-related decisions, the primacy of the human person shall be preserved. This principle is grounded in the University's founding conviction that education is fundamentally about forming people of excellence and integrity for service.

This principle has practical implications. No student shall be subjected to a purely automated decision that produces legal or similarly significant effects without meaningful human review, consistent with the Nigeria Data Protection Act 2023. No academic staff member shall be replaced by an AI system in matters requiring professional judgment, academic mentorship, or the assessment of character. Administrative AI applications shall function as decision-support tools, not autonomous decision-makers.

5.2 Academic Integrity

McPherson University's commitment to academic integrity is non-negotiable. AI shall not be used to misrepresent original work, bypass assessment, or undermine the University's standards of scholarly honesty. At the same time, the University recognises that AI literacy is now an essential component of higher education, and that legitimate AI-assisted learning must be distinguished from academic misconduct.

This principle requires a nuanced approach. The University does not prohibit AI use. It regulates it. Students and staff must understand the difference between AI-assisted work — where the human author retains primary creative and analytical responsibility — and AI-generated content produced substantially or entirely by an AI system. The University's approach to academic integrity in the AI context is detailed in Section 8.

5.3 Transparency and Disclosure

AI use in academic work, research, and administrative processes shall be transparent and, where required, disclosed. The University community must be able to understand when, how, and to what extent AI has contributed to a particular output or decision. Transparency requirements shall be graduated according to context: more extensive disclosure for research publications, moderate disclosure for coursework, and appropriate disclosure for administrative applications.

The University affirms that concealment of AI use in contexts where disclosure is required constitutes a breach of this policy. However, the University also recognises that over-disclosure can be burdensome and unnecessary. The specific disclosure requirements for each context are set out in Sections 8, 9, and 12.

5.4 Accountability

Clear lines of accountability shall exist for all AI-related decisions and outcomes. Every AI system deployed by the University shall have a named responsible officer or unit. Every AI-related decision that affects a student or staff member shall be traceable to a human decision-maker who retains ultimate responsibility. The University rejects the notion that responsibility can be diffused or diminished by the involvement of an AI system.

This principle extends to third-party AI tools. Where the University procures or approves an AI service, accountability for its responsible use remains with the University, notwithstanding the involvement of an external vendor. Vendor agreements shall include provisions that enable the University to meet its accountability obligations under this policy and Nigerian law.

5.5 Equity and Inclusion

AI shall not disadvantage any student or staff member on the basis of gender, age, ethnicity, religion, disability, socio-economic background, or any other protected characteristic. The University is particularly attentive to algorithmic bias, which can arise from training data that does not reflect the diversity of the University community or the Nigerian context.

The University commits to evaluating AI tools for bias before adoption, monitoring deployed systems for disparate impact, and providing accessible alternatives where AI-enabled systems create barriers. This principle also requires attention to the digital divide within the University community. No student shall be academically disadvantaged because they lack access to AI tools that are permitted or encouraged in a particular course. Where AI tools are recommended, the University shall ensure equitable access through institutional licences, campus facilities, or alternative arrangements.

5.6 Privacy and Data Protection

All AI-related processing of personal data shall comply with the Nigeria Data Protection Act 2023 and its General Application and Implementation Directive 2025. The University shall process personal data lawfully, fairly, and transparently. Personal data shall be collected for specified, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes.

The University shall conduct Data Privacy Impact Assessments before deploying AI systems that process personal data. The University's designated Data Protection Officer shall be consulted on all AI procurement and deployment decisions that involve personal data. The specific data protection provisions applicable to AI at McPherson University are detailed in Sections 19 to 21.

5.7 Security and Reliability

AI systems deployed by the University shall be secure, resilient, and dependable. The University shall implement appropriate technical and organisational measures to protect AI systems from unauthorised access, manipulation, or disruption. AI systems that support critical University functions — such as admissions, examination administration, or financial management — shall be subject to enhanced security and reliability requirements.

The University also recognises that AI systems can themselves be used as instruments of cyberattack, including through deepfakes, automated social engineering, and adversarial manipulation. This policy

therefore incorporates provisions for AI-related cybersecurity awareness, incident response, and the prohibition of malicious AI use, as detailed in Section 23.

5.8 Stewardship of Institutional Values

McPherson University is a faith-based institution founded by the Foursquare Gospel Church in Nigeria. Its mission is to provide education "with Godly virtues that will prepare men and women for leadership and positive impact on society". AI governance at the University must be consistent with this mission.

This principle requires that AI use at McPherson University be evaluated not only against technical, legal, and pedagogical criteria, but also against the University's foundational commitments to honesty, stewardship, human dignity, and the common good. The University does not adopt AI uncritically. It adopts AI that serves its mission. Where an AI application would compromise the University's values, it shall be rejected, regardless of its technical sophistication or efficiency gains.

The University also affirms that its Christian identity is not a barrier to technological engagement but a foundation for it. The University's heritage calls it to be a steward of knowledge, a servant of society, and a community of integrity. AI, responsibly governed, can serve these ends.

5.9 Continuous Learning

The rapid evolution of AI requires that the University community be equipped for ongoing learning and adaptation. AI literacy shall not be a one-time training exercise but a continuous commitment. The University shall invest in building the AI competencies of its staff and students, as detailed in Sections 26 and 27.

This principle also applies to the policy itself. The University acknowledges that AI governance is a moving target. This policy shall be reviewed regularly, and the University shall remain attentive to emerging AI developments, changing regulatory requirements, and the evolving needs of its community.

5.10 Proportionality

AI governance measures shall be commensurate with the risks associated with particular AI applications. Low-risk AI uses — such as using a grammar checker or a scheduling assistant — shall not be subject to the same level of scrutiny as high-risk uses — such as AI systems that affect student assessment, admissions, or disciplinary outcomes.

The University shall adopt a risk-tiered approach to AI governance, with differentiated requirements for different categories of AI use. This principle ensures that the policy is both rigorous and practical, protecting the University from harm without imposing unnecessary burdens that would inhibit legitimate innovation and productivity.

Section 6: Alignment with National Regulatory Framework

6.1 The NUC Artificial Intelligence Policy Framework

The National Universities Commission has developed the Artificial Intelligence Policy Framework and Implementation Roadmap for the Nigerian University System, providing a structured framework for responsible AI integration. The NUC's framework emphasises retaining human judgment in accreditation and licensing decisions, integrating AI competencies and ethics across disciplines under the Core

Curriculum and Minimum Academic Standards (CCMAS), and ensuring that AI adoption serves academic quality rather than replacing it.

McPherson University aligns fully with the NUC framework. This policy has been developed to operationalise the NUC's guidance at the institutional level. Specifically, the University commits to:

- (a) Retaining human judgment in all academic and administrative decisions, including accreditation, licensing, and disciplinary matters;
- (b) Integrating AI competencies and ethics into its curriculum across all Colleges, in alignment with the CCMAS framework;
- (c) Participating in the NUC's periodic monitoring of AI development in universities, using the NUC's standardised reporting template;
- (d) Engaging with the NUC's programmes for enhanced human capacity development on AI; and
- (e) Reporting AI-related developments and compliance to the NUC as required.

6.2 Integration of AI Competencies Under CCMAS

The NUC has approved the inclusion of Artificial Intelligence as a programme in the Core Curriculum and Minimum Academic Standards, with universities directed to commence implementation from the 2025/2026 academic session subject to successful resource assessment. The NUC has also emphasised that AI competencies and ethics should be integrated across disciplines, not confined to computing programmes alone.

McPherson University recognises this dual expectation. The University shall pursue two complementary strategies: first, it shall evaluate the feasibility of introducing a dedicated programme in Artificial Intelligence or related fields, subject to resource assessment and Senate approval; second, it shall integrate AI literacy and ethics into the curriculum of all existing programmes, ensuring that every McPherson University graduate — regardless of discipline — possesses foundational AI competence and ethical awareness.

6.3 The Nigeria National Artificial Intelligence Strategy 2025–2029

The Nigeria National Artificial Intelligence Strategy (NAIS), published in September 2025, sets a five-year vision to position Nigeria as a global leader in ethical and inclusive AI innovation. The Strategy is organised around three goals: economic growth and competitiveness, social development and inclusion, and technological advancement and leadership. Its five operational pillars include building foundational AI infrastructure, building a world-class AI ecosystem, accelerating AI adoption across key sectors, ensuring responsible and ethical AI, and developing a robust governance framework.

McPherson University aligns with NAIS and commits to contributing to its objectives within the University's sphere of influence. In particular:

- (a) **AI infrastructure.** The University shall continue to strengthen its ICT infrastructure to support AI-related teaching, learning, and research, recognising that reliable infrastructure is a precondition for meaningful AI adoption.

(b) **AI talent.** The University shall contribute to NAIS's target of equipping at least 70% of Nigeria's young workforce aged 16–35, including 50% women, with AI-related skills. McPherson University shall work towards ensuring that its graduates possess AI competencies relevant to their disciplines.

(c) **Responsible and ethical AI.** The University shall participate in the national conversation on AI ethics, contributing its distinctive perspective as a faith-based institution committed to human dignity and the common good.

(d) **AI governance.** The University shall comply with NAIS's governance requirements, including the National AI Risk Management Framework, to the extent applicable to university operations.

6.4 The Nigeria Data Protection Act 2023

The Nigeria Data Protection Act 2023 (NDPA) is the principal legislation governing the processing of personal data in Nigeria. The NDPA establishes the Nigeria Data Protection Commission, sets out principles for lawful data processing, and creates enforceable rights for data subjects. Of particular relevance to AI governance is Section 37 of the NDPA, which guarantees data subjects the right not to be subjected to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects.

McPherson University shall comply fully with the NDPA. The University shall process personal data in accordance with the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality. The University's specific obligations under the NDPA, including the appointment of a Data Protection Officer, the conduct of Data Privacy Impact Assessments, and the handling of data subject rights, are detailed in Section 19.

The University notes that Section 37 of the NDPA does not prohibit all automated decision-making. It restricts decisions that are based solely on automated processing and that produce legal or similarly significant effects. The University shall ensure that all AI-assisted decisions affecting students or staff include meaningful human oversight, and that data subjects are informed of their rights under the NDPA.

6.5 The Nigeria Data Protection Act General Application and Implementation Directive 2025

The General Application and Implementation Directive 2025 (GAID) issued by the Nigeria Data Protection Commission provides detailed operational guidance on the implementation of the NDPA. The GAID introduces provisions specifically addressing the deployment of emerging technologies, including artificial intelligence, in personal data processing.

McPherson University shall comply with the GAID. This includes adopting interoperable data privacy measures where AI systems process personal data, conducting privacy impact assessments for high-risk processing, and ensuring that AI systems are designed and deployed in a manner that protects data subject rights.

6.6 The Cybercrimes (Amendment) Act 2024

The Cybercrimes (Amendment) Act 2024 establishes the legal framework for combating cybercrime in Nigeria, including offences related to unauthorised access to computer systems, data interference, and the use of computer systems for fraudulent purposes. AI systems can be used to commit or facilitate cybercrimes, and the University must ensure that its AI deployments do not create vulnerabilities or facilitate criminal activity.

McPherson University shall comply with the Cybercrimes (Amendment) Act 2024. The University shall implement appropriate cybersecurity measures for AI systems, prohibit the use of AI for malicious purposes, and cooperate with law enforcement authorities in the investigation of AI-related cybercrimes. Specific provisions are detailed in Section 23.

6.7 The Nigerian Ethical AI Framework

The Nigerian Ethical AI Framework (NEAIF) is an independently developed ethical governance framework for AI in Nigeria, designed to complement the National AI Strategy. NEAIF addresses gaps in the national framework by focusing on data sovereignty, bias mitigation, transparency requirements, and accountability mechanisms, while remaining compatible with international standards such as the OECD AI Principles and UNESCO's Recommendation on the Ethics of AI.

McPherson University commends the NEAIF's emphasis on practical, culturally grounded, and enforceable ethical governance. The University shall draw on NEAIF's principles in the development of its own AI governance practices, particularly in relation to data sovereignty (ensuring that Nigerian data serves Nigerian development priorities), bias mitigation (evaluating AI systems for algorithmic discrimination), and accountability (maintaining clear human responsibility for AI outcomes).

6.8 NUC Compliance Monitoring and Reporting

The NUC has committed to enforcing compliance with its AI policy framework through rigorous, periodic monitoring of individual university AI development using a standardised reporting template. McPherson University shall participate fully in this monitoring process. The University's AI Policy Committee (established under Section 29.3) shall be responsible for preparing and submitting the University's AI compliance reports to the NUC.

The University shall maintain records of AI systems deployed, AI-related training conducted, AI policies and procedures, and AI incidents reported. These records shall be available for NUC inspection upon request. The University views NUC monitoring not as an external imposition but as a constructive mechanism for institutional learning and improvement.

Section 7: Alignment with International Best Practice

7.1 UNESCO Recommendation on the Ethics of Artificial Intelligence

The UNESCO Recommendation on the Ethics of AI, adopted by all UNESCO member states in 2021, is the most widely endorsed international standard for AI ethics. It affirms that AI should be developed and used in ways that respect human dignity, human rights, and fundamental freedoms. It emphasises the importance of ethical impact assessments, meaningful human oversight, and the protection of vulnerable groups.

McPherson University aligns with the UNESCO Recommendation. The University's principles of human-centred governance, equity, and transparency (Sections 5.1, 5.5, and 5.3) are consistent with UNESCO's ethical framework. The University shall apply UNESCO's guidance in the evaluation of AI tools and in the development of AI-related curricula.

7.2 OECD AI Principles

The OECD AI Principles, adopted in 2019 and updated in 2024, provide a global standard for responsible AI stewardship. They affirm that AI should benefit people and the planet, respect human rights and democratic values, be transparent and explainable, function robustly and safely, and be subject to accountability.

McPherson University aligns with the OECD AI Principles. The University's commitment to accountability (Section 5.4), security and reliability (Section 5.7), and transparency (Section 5.3) reflects OECD guidance. The University shall draw on OECD's risk management framework in developing its own AI risk assessment processes (Section 24).

7.3 Comparative Approaches from Leading University AI Policies

The University has reviewed AI policies adopted by peer institutions in Nigeria and internationally. This review has informed the development of this policy, ensuring that McPherson University's approach reflects emerging best practice while remaining tailored to its distinctive mission and context.

The University notes in particular the "Humanitas AI Compact" adopted by certain faith-based institutions, which commits signatories to principles including human dignity, subsidiarity, the common good, truth, and the integral development of the person. McPherson University shares these commitments and shall seek opportunities to collaborate with other institutions that are developing ethical AI governance frameworks consistent with their institutional values.

7.4 McPherson University's Distinctive Contribution

McPherson University approaches AI governance not as a late adopter seeking to catch up with global trends, but as an institution with a distinctive contribution to make. The University's identity as a faith-based institution committed to excellence, integrity, and service positions it to articulate an approach to AI governance that integrates technological competence with moral formation.

The University's contribution to the Nigerian and African AI governance conversation shall be characterised by three distinctive emphases:

First, a commitment to human dignity as the foundation of AI ethics. McPherson University affirms that human beings are not merely data points or consumers of AI outputs. They are persons endowed with dignity, created for relationship with God and neighbour. AI governance must begin from this foundational conviction.

Second, a commitment to the common good. The University rejects approaches to AI that serve narrow interests at the expense of the broader society. AI adoption at McPherson University shall be evaluated by its contribution to the flourishing of the University community, Nigerian society, and the African continent.

Third, a commitment to integrity in a digital age. As AI makes it easier to generate plausible content and automate complex processes, the temptations to deceive, cut corners, and exploit others increase. McPherson University shall be a community that models integrity in its use of AI, demonstrating that technological sophistication and moral seriousness are not adversaries but partners.

Part Three: AI in Teaching, Learning, and Assessment

Section 8: AI and Academic Integrity

8.1 Foundational Position

McPherson University's approach to AI and academic integrity is governed by a single, unambiguous conviction: **the University exists to form people of excellence and integrity for service.** This conviction, drawn directly from the University's founding vision, cannot be reconciled with any practice that allows a student to misrepresent the work of a machine as the work of a human mind, or that permits a member of the academic community to bypass the intellectual labour that constitutes genuine learning.

At the same time, McPherson University rejects the false choice between prohibiting AI altogether and permitting its unrestricted use. The University recognises that AI literacy is now an essential graduate competency, that AI tools are embedded in professional practice across every discipline the University teaches, and that students who are denied guided exposure to these tools will be disadvantaged in the labour market. The University's approach is therefore regulatory, not prohibitive. It distinguishes between legitimate AI-assisted learning and academic misconduct, and it holds students accountable for understanding the difference.

8.2 Definition of Academic Misconduct in the AI Context

For the purposes of this policy, academic misconduct involving AI includes, but is not limited to:

- (a) **Contract cheating by proxy.** Submitting work generated substantially or entirely by an AI system as one's own original work, where the assessment requires independent student authorship.
- (b) **Unauthorised content generation.** Using AI to generate essays, reports, code, designs, laboratory analyses, or other assessable outputs where the course or assessment explicitly prohibits such use.
- (c) **Concealment of required disclosure.** Failing to disclose AI use where this policy or a course-level guideline requires disclosure.
- (d) **Fabrication of sources.** Using AI to generate fake citations, references, data, or quotations, whether or not the AI system was prompted to do so.
- (e) **Impersonation in assessment.** Using AI to simulate the student's voice, reasoning, or knowledge in an examination, oral assessment, or other context where the student's own understanding is being assessed.
- (f) **Unauthorised assistance in examinations.** Using AI tools during closed-book or invigilated examinations, or in any assessment context where AI use is prohibited.
- (g) **Facilitating misconduct by others.** Providing AI-generated work to another student for submission, or assisting another student in using AI to commit academic misconduct.
- (h) **Manipulation of AI detection.** Intentionally using tools or techniques designed to evade AI detection in circumstances where disclosure was required.

8.3 Permitted Uses of AI in Academic Work

The following uses of AI are generally permitted, subject to course-level guidance and the disclosure requirements in Section 8.4:

- (a) **Research and information gathering.** Using AI to locate, summarise, or organise publicly available information, provided the student verifies the accuracy and reliability of AI outputs through independent sources.
- (b) **Brainstorming and ideation.** Using AI to generate ideas, outline structures, or explore alternative approaches to a problem, provided the student exercises independent judgment in selecting and developing those ideas.
- (c) **Language and writing support.** Using AI for grammar checking, style suggestions, translation assistance, or vocabulary enhancement, provided the substantive content and argumentation remain the student's own.
- (d) **Study and revision.** Using AI for practice questions, concept explanation, or self-assessment, provided the student does not present AI-generated answers as their own work in formal assessments.
- (e) **Data analysis support.** Using AI tools to assist with statistical analysis, coding, or data visualisation, provided the student understands and can explain the methods used and the results obtained.
- (f) **Accessibility support.** Using AI tools to support learning where a student has a documented disability or learning difference, in accordance with approved accommodation arrangements.

8.4 Disclosure Requirements

The University adopts a graduated disclosure approach, calibrated to the nature of the assessment and the extent of AI use:

Level One — No Disclosure Required. Use of AI for study support, grammar checking, or brainstorming, where the AI output does not appear in the submitted work.

Level Two — Brief Disclosure Required. Use of AI for language editing, translation, or minor structural suggestions, where the student's substantive work remains dominant. Disclosure may take the form of a brief statement in the assessment cover sheet.

Level Three — Detailed Disclosure Required. Use of AI for research assistance, data analysis, or content generation that has materially shaped the submitted work. Disclosure shall include the AI tool used, the purpose of use, the prompts or instructions given, and the extent to which AI output was incorporated.

Level Four — Explicit Authorisation Required. Use of AI in contexts where the course or assessment defaults to prohibition. Explicit authorisation must be obtained from the course lecturer in advance, and detailed disclosure shall be required.

The specific disclosure requirements for research and publication are addressed separately in Section 12.4.

8.5 Course-Level AI Guidelines

Every course at McPherson University shall have an explicit AI use statement in its syllabus or course guide. This statement shall:

- (a) Specify the category of AI use permitted for the course, using the five-category scale in Section 9.2;
- (b) Identify any specific AI tools that are approved or prohibited for the course;
- (c) Explain the disclosure requirements applicable to the course;

- (d) Provide examples of permissible and impermissible AI use in the context of the discipline;
- (e) State the consequences of non-compliance.

Course lecturers are responsible for preparing these statements, subject to review by the Head of Department and the Dean of the College. The AI Policy Committee shall provide templates and guidance to support lecturers in fulfilling this responsibility.

8.6 Detection and Investigation of AI-Related Misconduct

The University recognises that reliable detection of AI-generated content is an emerging and imperfect science. No single detection tool shall be treated as conclusive evidence of misconduct. Instead, the University adopts a multi-evidence approach:

- (a) **Detection tools.** AI detection software may be used as one source of evidence, but its output shall not, by itself, establish misconduct.
- (b) **Substantive review.** Academic staff shall assess submitted work against the student's known capabilities, prior submissions, and the requirements of the assessment.
- (c) **Oral verification.** Where AI-related misconduct is suspected, the student may be required to explain, defend, or reproduce their work orally. Refusal to participate in such verification shall be treated as an aggravating factor.
- (d) **Process evidence.** Records of AI tool usage, version histories, and draft materials may be considered where available and lawfully obtained.
- (e) **Investigative procedure.** All allegations of AI-related misconduct shall be investigated in accordance with the University's established academic misconduct procedures, with full respect for the student's right to respond to allegations and to be heard.

8.7 Penalties and Remediation

Penalties for AI-related academic misconduct shall be proportionate to the nature and severity of the offence, and shall be consistent with the University's existing academic misconduct regulations. Penalties may include:

- (a) **Warning and resubmission** for minor or first-time offences involving negligence rather than intent.
- (b) **Mark reduction or capped resubmission** for offences involving unauthorised AI use without aggravating factors.
- (c) **Failure of the assessment or course** for serious offences or repeat offences.
- (d) **Suspension or expulsion** for egregious offences, including contract cheating, examination impersonation, or systematic misconduct.

The University shall also provide **remediation and education** where appropriate. Students found to have committed AI-related misconduct shall be required to complete an academic integrity education module before resuming normal academic standing.

8.8 Appeals and Due Process

Students accused of AI-related academic misconduct shall have the right to:

- (a) Be informed in writing of the specific allegations against them;
- (b) Review the evidence relied upon by the University;
- (c) Respond to the allegations, including by submitting their own evidence;
- (d) Be accompanied by a representative or advisor at any disciplinary hearing;
- (e) Appeal any adverse decision through the University's established appeals procedures;
- (f) Have the matter heard within a reasonable time.

The University affirms that the presumption of innocence applies to all academic misconduct proceedings, including those involving AI.

8.9 Staff Academic Integrity Obligations

Academic integrity obligations under this policy apply equally to academic staff. Staff shall not:

- (a) Use AI to generate course materials, lecture notes, or assessment instruments without disclosure and appropriate quality assurance;
- (b) Use AI to produce research outputs without following the disclosure requirements in Section 12;
- (c) Use AI to assess student work without human review and judgment;
- (d) Misrepresent AI-generated work as their own in any academic or professional context.

Section 9: Course-Level AI Guidelines

9.1 Faculty Responsibility

Every academic staff member at McPherson University is responsible for defining the parameters of permissible AI use within the courses they teach. This responsibility is not delegable. Faculty members are best positioned to understand the learning objectives of their courses, the nature of the assessments they design, and the disciplinary standards that apply to student work.

The University provides the following framework to guide faculty in the exercise of this responsibility. The framework is designed to be sufficiently flexible to accommodate the diversity of disciplines, pedagogies, and assessment methods across the University's five Colleges, while ensuring consistency and clarity for students.

9.2 The Five-Category AI Use Scale

The University adopts a five-category scale to describe the level of AI use permitted in a course or assessment. Faculty shall select the appropriate category for each course and, where relevant, for individual assessments within a course.

Category 1 — No AI Permitted. AI tools of any kind are prohibited for the completion of the assessment. This category applies to assessments that test foundational knowledge, closed-book examinations, invigilated assessments, and any context where the student's unaided capability is being assessed.

Category 2 — AI for Preparation Only. AI may be used for study, revision, and preparation, but not for the generation of the submitted work. This category applies to traditional essays, problem sets, and assessments where students are expected to demonstrate independent analytical or creative work.

Category 3 — AI as Language and Structure Support. AI may be used for grammar, spelling, punctuation, translation, and stylistic suggestions, but not for the generation of substantive content, arguments, or analysis. The student's intellectual contribution must remain dominant.

Category 4 — AI as Research and Analysis Assistant. AI may be used for research assistance, data analysis, coding support, or the generation of draft materials that the student then substantially rewrites, critiques, and develops. Detailed disclosure is required.

Category 5 — AI-Integrated Work. AI is a permitted and expected component of the work, with students required to document their AI use and critically evaluate the AI outputs as part of the assessment. This category applies to courses where AI literacy is an explicit learning outcome, or where the assessment is designed to test the student's ability to work effectively with AI.

9.3 Syllabus Statements on AI Use

Every course syllabus shall include an AI use statement. The statement shall be concise and accessible to students, and shall specify:

- (a) The AI use category or categories applicable to the course;
- (b) The specific tools that are approved, prohibited, or unrestricted;
- (c) The disclosure requirements that apply;
- (d) The consequences of non-compliance;
- (e) Where students can seek clarification or support.

The AI Policy Committee shall publish a model syllabus statement that faculty may adapt to their disciplines.

9.4 Assignment-Level AI Use Mapping

Within a course, different assessments may warrant different AI use categories. For example, a course may permit AI for a research essay (Category 4) but prohibit it for a final examination (Category 1). Faculty shall therefore map AI use categories to individual assessments, and shall communicate this mapping clearly to students at the beginning of the course.

9.5 Disclosure Requirements for AI-Assisted Work

Where disclosure is required, students shall complete an AI Use Disclosure Form (provided in Appendix B) for the relevant assessment. The form shall require the student to:

- (a) Identify the AI tool(s) used;
- (b) Describe the purpose of use;
- (c) Summarise the prompts or instructions given;
- (d) Explain how the AI output was incorporated into the submitted work;
- (e) Confirm that the student has reviewed and takes responsibility for the accuracy and integrity of the final submission.

Faculty may also require a Reflective AI Use Statement (Appendix C) for assessments in Categories 4 and 5, in which the student reflects critically on the role of AI in their learning process and the strengths and limitations of the AI tools used.

9.6 Citation and Attribution Standards for AI-Generated Content

Where AI-generated content is incorporated into submitted work, students shall cite it in accordance with disciplinary conventions. The University adopts the principle that AI tools are not authors and cannot be listed as authors in any academic work. Instead, AI use shall be acknowledged in the methodology, acknowledgements, or a dedicated disclosure statement, as appropriate to the discipline.

The University shall publish discipline-specific citation guidance in collaboration with the University Library. Where disciplinary conventions are unsettled, students shall follow the general principle of full, honest, and transparent disclosure.

9.7 Verification and Fact-Checking Requirements

Students are responsible for the accuracy of all work they submit, regardless of the source of any content. Where AI tools have been used, students shall:

- (a) Verify all factual claims against reliable sources;
- (b) Confirm the existence and accuracy of all cited sources;
- (c) Check AI-generated data, calculations, and analyses for correctness;
- (d) Correct any errors or hallucinations in AI outputs before submission.

Failure to verify AI-generated content, resulting in the submission of false or misleading material, shall be treated as academic misconduct.

9.8 Accommodations for Students with Disabilities

Students with documented disabilities or learning differences may use AI tools as part of approved accommodation arrangements. The University's Disability Support Office shall assess accommodation requests involving AI on a case-by-case basis, in consultation with the student, the course lecturer, and where appropriate, the AI Policy Committee. Accommodations shall be designed to ensure equitable access to learning without compromising the integrity of assessment.

9.9 Equity Considerations in AI-Enabled Assessment

The University recognises that students have unequal access to AI tools. Some students may have personal subscriptions to premium AI services; others may rely solely on free or institutional tools. Some may have unreliable internet access or limited data. Some may lack the digital literacy to use AI tools effectively.

Faculty shall therefore:

- (a) Avoid assessments that assume access to paid AI tools, unless the University provides equivalent access;
- (b) Ensure that where AI use is required, institutional tools are made available;
- (c) Provide alternatives for students who cannot access required AI tools;
- (d) Avoid penalising students for lacking prior AI experience, and instead provide instruction and support.

Section 10: AI Literacy and Student Development

10.1 Embedding AI Literacy Across All Programmes

McPherson University commits to ensuring that every graduate, regardless of discipline, possesses foundational AI literacy. This commitment is consistent with the NUC's direction that AI competencies and ethics be integrated across disciplines under the CCMAS framework, and with the Nigeria National Artificial Intelligence Strategy's target of equipping a substantial proportion of Nigeria's young workforce with AI skills.

AI literacy at McPherson University is not limited to technical skills. It encompasses:

- (a) **Conceptual understanding** of what AI is, how it works, and what it can and cannot do;
- (b) **Critical evaluation** of AI outputs, including recognition of bias, hallucination, and limitation;
- (c) **Ethical reasoning** about the appropriate and inappropriate uses of AI;
- (d) **Practical competence** in using AI tools effectively and responsibly;
- (e) **Disciplinary application** of AI within the student's field of study.

10.2 University-Wide AI Literacy Requirement

The University shall introduce a foundational AI literacy component that is compulsory for all undergraduate students, delivered within the first two years of study. This component may take the form of a standalone course, an embedded module within General Studies, or a distributed set of learning experiences across multiple courses. The precise modality shall be determined by the Senate on the recommendation of the AI Policy Committee and the Committee of Deans.

For postgraduate students, AI literacy shall be integrated into research methodology training and discipline-specific coursework. Postgraduate students shall also receive training in the ethical use of AI in research and publication.

10.3 Critical Evaluation of AI Outputs

A central objective of AI literacy at McPherson University is the development of critical evaluation skills. Students shall be taught to:

- (a) Recognise when AI outputs are unreliable, biased, or fabricated;
- (b) Cross-check AI-generated information against authoritative sources;
- (c) Understand the limitations of AI systems, including knowledge cut-offs, training data biases, and hallucination tendencies;
- (d) Evaluate the ethical implications of AI outputs and applications;
- (e) Distinguish between AI capability and AI reliability.

10.4 Ethical Reasoning About AI

Students shall be equipped to reason ethically about AI use. This includes understanding:

- (a) The difference between AI-assisted and AI-generated work;

- (b) The importance of honesty and transparency in AI use;
- (c) The ethical implications of algorithmic bias and discrimination;
- (d) The privacy and data protection issues raised by AI;
- (e) The broader social and economic impacts of AI adoption;
- (f) The University's distinctive ethical commitments as a faith-based institution, including the dignity of the human person and the common good.

10.5 Prompt Engineering and Effective AI Collaboration

Students shall receive practical instruction in effective AI use, including:

- (a) Formulating clear and precise prompts;
- (b) Iterating and refining AI interactions;
- (c) Evaluating and selecting among AI outputs;
- (d) Integrating AI outputs with human judgment and creativity;
- (e) Documenting AI use for academic and professional purposes.

10.6 Understanding Algorithmic Bias and Limitations

Students shall learn to recognise and critically assess algorithmic bias, including:

- (a) Sources of bias in training data;
- (b) Manifestations of bias in AI outputs;
- (c) The disproportionate impact of biased AI on marginalised groups;
- (d) Strategies for mitigating and correcting bias.

This component of AI literacy is particularly important for students in health sciences, law, social sciences, and education, where AI-driven decisions can have significant consequences for individuals and communities.

10.7 Preparing Graduates for AI-Augmented Workplaces

McPherson University graduates will enter workplaces where AI tools are increasingly embedded in professional practice. The University's AI literacy programme shall therefore include:

- (a) Discipline-specific AI applications and tools;
- (b) Professional and regulatory standards for AI use in the student's field;
- (c) Collaboration with AI systems in professional workflows;
- (d) Leadership in responsible AI adoption;
- (e) Lifelong learning strategies for keeping pace with AI developments.

10.8 Co-Curricular AI Learning Opportunities

In addition to formal curricular provision, the University shall support co-curricular AI learning through:

- (a) AI-focused student clubs and societies;
- (b) Hackathons, competitions, and projects;
- (c) Guest lectures and industry engagement;
- (d) Online micro-credentials and short courses;
- (e) Peer learning and mentoring programmes.

The University Library shall curate AI learning resources accessible to all students.

Section 11: Faculty and Teaching Staff Responsibilities

11.1 Designing AI-Resilient Assessments

Faculty at McPherson University are responsible for designing assessments that are resilient to misuse while remaining valid and fair. AI-resilient assessment design includes:

- (a) Prioritising assessments that require original analysis, synthesis, or application rather than information reproduction;
- (b) Incorporating authentic, contextual, and discipline-specific tasks;
- (c) Using a mix of assessment formats, including oral examinations, presentations, and practical demonstrations where appropriate;
- (d) Designing assessments that require students to reflect on their process, not merely their product;
- (e) Sequencing assessments to allow for iterative feedback and revision.

The AI Policy Committee shall provide guidance and examples of AI-resilient assessment design across disciplines.

11.2 Modelling Responsible AI Use

Faculty shall model responsible AI use in their own teaching and professional practice. This includes:

- (a) Disclosing their own AI use in course materials and communications where relevant;
- (b) Demonstrating critical evaluation of AI outputs;
- (c) Discussing AI-related ethical dilemmas with students;
- (d) Acknowledging the limitations of AI tools in their disciplines;
- (e) Using AI to enhance teaching and learning, not to replace pedagogical judgment.

11.3 Providing Clear Guidance to Students

Faculty shall provide clear, timely, and accessible guidance to students on AI use. This includes:

- (a) Including AI use statements in course syllabi as required by Section 9.3;
- (b) Explaining the rationale for AI use categories and restrictions;
- (c) Providing examples of permissible and impermissible AI use;
- (d) Being available to answer student questions about AI use;

- (e) Ensuring that guidance is consistent across assessments within a course.

11.4 Ongoing Professional Development in AI Pedagogy

Faculty shall engage in ongoing professional development to maintain and enhance their AI pedagogical competence. The University shall provide:

- (a) Induction training on AI pedagogy for new faculty;
- (b) Regular workshops and seminars on AI developments, tools, and ethical issues;
- (c) Discipline-specific AI training and resources;
- (d) Opportunities for faculty to share best practices in AI integration;
- (e) Support for faculty to conduct research on AI in their disciplines.

11.5 Reporting AI-Related Concerns

Faculty shall report to the appropriate authority any AI-related concerns, including:

- (a) Suspected AI-related academic misconduct;
- (b) Unreliable or harmful AI tools;
- (c) AI-related security or privacy incidents;
- (d) Gaps or ambiguities in University AI policy;
- (e) Emerging AI developments that may require policy attention.

Reports shall be made to the Head of Department, Dean, or AI Policy Committee as appropriate, and shall be handled in accordance with the University's established reporting and whistleblower protections.

11.6 Balancing Innovation with Integrity

Faculty are encouraged to innovate in their use of AI for teaching and learning. Innovation shall be balanced with integrity, meaning that faculty shall:

- (a) Pilot new AI applications in low-stakes contexts before scaling;
- (b) Evaluate the pedagogical impact of AI tools, not merely their novelty;
- (c) Avoid adopting AI tools that compromise privacy, equity, or academic standards;
- (d) Document and share lessons learned from AI experimentation;
- (e) Be willing to discontinue AI practices that prove ineffective or harmful.

Part Four: AI in Research and Scholarship

Section 12: AI in Research

12.1 Foundational Position

McPherson University affirms that research and scholarship are central to its mission of providing qualitative, functional, and sound education. The University's vision of building "a people of excellence and integrity for service" extends to its research enterprise: McPherson University researchers are called not merely to produce knowledge, but to produce knowledge with integrity, rigour, and accountability.

Artificial Intelligence presents both extraordinary opportunities and genuine risks for research. AI can accelerate literature discovery, enhance data analysis, generate hypotheses, and assist with the mechanical aspects of scholarly writing. At the same time, AI can facilitate fabrication, undermine reproducibility, obscure the boundaries of authorship, and introduce bias into research findings. This policy seeks to harness AI's research potential while safeguarding the integrity upon which credible scholarship depends.

The University's approach to AI in research is guided by three principles. **First**, the researcher bears ultimate responsibility for all aspects of their work, regardless of the role played by AI. **Second**, the use of AI in research shall be disclosed transparently and in accordance with disciplinary and funder requirements. **Third**, AI shall be used to enhance, not substitute for, the intellectual labour that constitutes genuine scholarly contribution.

12.2 Permitted Uses of AI in Research

The following uses of AI in research are generally permitted, subject to the disclosure requirements in Section 12.4 and any applicable funder or publisher requirements:

- (a) **Literature discovery and review.** Using AI tools to identify, summarise, and organise relevant literature, provided the researcher independently verifies the accuracy of AI-generated summaries and cites primary sources correctly.
- (b) **Data analysis and visualisation.** Using AI to assist with statistical analysis, pattern recognition, coding, and data visualisation, provided the researcher understands the methods used and can explain the results obtained.
- (c) **Hypothesis generation and research design.** Using AI to explore potential research questions, generate hypotheses, or suggest methodological approaches, provided the researcher exercises independent judgment in selecting and developing research directions.
- (d) **Writing and editing support.** Using AI for language editing, grammar checking, style improvement, and translation assistance, provided the substantive content, argumentation, and interpretation remain the researcher's own.
- (e) **Simulation and modelling.** Using AI to create simulations, models, or synthetic datasets for research purposes, where appropriate and clearly disclosed.
- (f) **Coding and software development.** Using AI to assist with programming, debugging, or software development for research purposes, provided the researcher understands and can explain the code produced.

(g) **Administrative and grant-writing support.** Using AI to assist with formatting, compliance checking, or administrative aspects of grant applications, provided all substantive content is the applicant's own.

12.3 Prohibited Uses of AI in Research

The following uses of AI in research are prohibited:

- (a) **Fabrication of data or results.** Using AI to generate false or misleading research data, results, or findings.
- (b) **Fabrication of sources.** Using AI to generate fake citations, references, or quotations, or citing AI-generated sources that do not exist.
- (c) **Undisclosed AI authorship of substantive content.** Presenting AI-generated text, analysis, or interpretation as the researcher's own original intellectual contribution.
- (d) **Plagiarism by AI proxy.** Using AI to reproduce or paraphrase the work of others without proper attribution.
- (e) **Manipulation of research integrity systems.** Using AI to circumvent plagiarism detection, peer review, or other research integrity mechanisms.
- (f) **Unauthorised use of human subjects data.** Using AI to analyse personal data from human research participants without appropriate ethical approval and data protection safeguards.
- (g) **Deceptive AI use in peer review or editorial processes.** Using AI to generate peer review reports or editorial decisions without disclosure, or using AI to manipulate these processes.

12.4 Disclosure and Attribution of AI Contributions to Research

The University adopts the following disclosure requirements for AI use in research:

Principle of Full Disclosure. Researchers shall disclose all AI use that has materially contributed to the research process, including in the methodology section, acknowledgements, or a dedicated AI disclosure statement, as appropriate to the discipline and publication venue.

Authorship Exclusion. AI systems shall not be listed as authors or co-authors of any research output. Authorship requires accountability that AI systems cannot provide. The human researcher(s) who used AI remain fully responsible for all aspects of the work.

Content Disclosure. Where AI-generated content appears in a research output — whether as text, data, code, images, or other material — the researcher shall clearly identify which components were AI-generated and describe how they were generated and verified.

Prompt Documentation. For research involving significant AI use, researchers shall maintain records of the prompts or instructions given to AI systems, sufficient to enable reproduction and verification of the research process. These records shall be made available to the Research Ethics Committee or to journal editors upon request.

Citation Conventions. Where disciplinary conventions for citing AI use exist, researchers shall follow them. Where conventions are unsettled, the University shall publish guidance in collaboration with the University Library and the Research Ethics Committee.

12.5 AI in Literature Review and Systematic Synthesis

AI tools are increasingly used in literature review and systematic synthesis. The University permits such use subject to the following safeguards:

- (a) **Search transparency.** Researchers shall document the AI tools used for literature searching, the databases and sources covered, and the search strategies employed.
- (b) **Source verification.** All citations in the final output shall be verified against the original sources. AI-generated citations shall not be relied upon without independent confirmation.
- (c) **Synthesis integrity.** Where AI is used to summarise or synthesise literature, the researcher shall critically evaluate the AI output against the source materials and take responsibility for the accuracy and completeness of the synthesis.
- (d) **Systematic review standards.** Systematic reviews and meta-analyses shall comply with relevant reporting standards, including disclosure of AI use where required.

12.6 AI in Data Collection and Processing

Researchers using AI for data collection or processing shall:

- (a) **Obtain appropriate ethical approval.** Where data involves human participants, AI-assisted data collection or processing shall be included in the ethical review application and approved by the Research Ethics Committee.
- (b) **Ensure data protection compliance.** AI processing of personal data shall comply with the Nigeria Data Protection Act 2023 and the University's Data Protection Policy, as detailed in Sections 19 to 21.
- (c) **Document processing methods.** The AI tools, algorithms, and processing steps used shall be documented sufficiently to enable reproducibility.
- (d) **Validate AI outputs.** AI-generated or AI-processed data shall be validated against independent sources or methods where feasible.
- (e) **Address bias.** Researchers shall assess AI systems for potential bias in data collection or processing and take reasonable steps to mitigate such bias.

12.7 AI in Experimental Design and Simulation

AI-assisted experimental design and simulation are permitted, subject to the following conditions:

- (a) **Methodological justification.** The use of AI in experimental design or simulation shall be methodologically justified and described in sufficient detail to enable replication.
- (b) **Validation.** AI-generated simulations or models shall be validated against empirical data or established theoretical expectations where possible.
- (c) **Limitations disclosure.** The limitations of AI-based methods shall be acknowledged in research outputs.
- (d) **Computational resources.** Researchers shall ensure that AI-based methods are computationally feasible and do not require resources beyond those reasonably available to the University.

12.8 Compliance with Funder and Journal Requirements

Researchers shall comply with all funder and journal requirements regarding AI use. Where funder or journal requirements are more stringent than this policy, the more stringent requirements shall prevail. Where funder or journal requirements are less stringent, this policy shall apply.

The University shall monitor developments in funder and journal AI policies and shall provide guidance to researchers on compliance. The Research Office shall maintain a repository of relevant policies from major funders and publishers.

12.9 Intellectual Property Considerations

(a) **Ownership.** The University's existing Intellectual Property Policy shall govern ownership of AI-assisted research outputs. Researchers shall consult the Research Office where questions arise regarding ownership of AI-generated or AI-assisted inventions or works.

(b) **Patentability.** Researchers shall be aware that AI-generated inventions may raise novel questions of patentability under Nigerian and international law. The Research Office shall provide guidance on these matters.

(c) **Licensing.** Where AI tools are used in research, researchers shall comply with the terms of any applicable licences, including restrictions on commercial use or redistribution of AI-generated outputs.

(d) **Third-party rights.** Researchers shall ensure that their use of AI does not infringe the intellectual property rights of others, including rights in training data.

Section 13: Research Ethics and AI

13.1 Ethical Review Requirements for AI-Related Research

All research involving AI that falls within the University's definition of research involving human participants, personal data, or potential harm shall be submitted for ethical review by the University Research Ethics Committee (REC). This includes:

- (a) Research that uses AI to collect, process, or analyse personal data.
- (b) Research that deploys AI systems in contexts affecting individuals or communities.
- (c) Research that develops or tests AI systems with potential for harm.
- (d) Research on AI itself, including studies of AI capabilities, limitations, and impacts.

The REC shall include among its members or advisors persons with expertise in AI ethics and data protection. Where the REC lacks such expertise, it shall seek external advice.

13.2 Protection of Human Subjects in AI Research

Research involving human participants and AI shall comply with all applicable ethical standards, including:

- (a) **Informed consent.** Participants shall be informed of any AI involvement in the research, including how their data will be used in AI systems, and shall provide informed consent.

(b) **Vulnerable populations.** Research involving vulnerable populations — including children, persons with disabilities, and economically disadvantaged persons — shall be subject to enhanced ethical scrutiny where AI is involved.

(c) **Right to withdrawal.** Participants shall retain the right to withdraw from AI-related research, including the right to request deletion of their data from AI systems where feasible.

(d) **Protection from harm.** Research shall be designed to minimise the risk of harm to participants from AI-related activities, including psychological, social, economic, or reputational harm.

13.3 Avoidance of Algorithmic Harm

Researchers shall take reasonable steps to avoid algorithmic harm, including:

(a) **Bias assessment.** Assessing AI systems for potential bias against individuals or groups based on protected characteristics.

(b) **Impact evaluation.** Evaluating the potential impacts of AI research on communities and individuals, particularly those in vulnerable situations.

(c) **Mitigation measures.** Implementing measures to mitigate identified risks of algorithmic harm.

(d) **Transparency.** Being transparent about the limitations and potential harms of AI systems used in research.

13.4 Data Sovereignty and Local Relevance

McPherson University affirms the principle of data sovereignty: the data generated by Nigerian researchers and institutions, and the data of Nigerian communities, should serve Nigerian and African development priorities. Researchers using AI shall:

(a) Prioritise research questions that address Nigerian and African development challenges;

(b) Ensure that research benefits accrue to Nigerian and African communities;

(c) Avoid extractive research practices that exploit Nigerian data without contributing to local capacity;

(d) Comply with Nigerian data protection law and any applicable data localisation requirements;

(e) Consider the ethical implications of transferring Nigerian data to foreign AI systems or jurisdictions.

13.5 Research on Africa-Priority Themes Using AI

The University encourages AI-assisted research on themes of particular relevance to Nigeria and Africa, including:

(a) **Health.** AI applications in malaria, tuberculosis, maternal health, and other priority health challenges.

(b) **Agriculture and food security.** AI applications in crop improvement, pest management, and food systems.

(c) **Education.** AI applications in teaching, learning, and educational access.

(d) **Governance and public administration.** AI applications in public service delivery, transparency, and accountability.

(e) **Climate and environment.** AI applications in climate modelling, environmental monitoring, and sustainable development.

(f) **Economic development.** AI applications in entrepreneurship, financial inclusion, and job creation.

Researchers pursuing AI-related research on these themes shall be eligible for University research funding and support, subject to available resources.

13.6 Collaborations with External AI Research Partners

Collaborations with external partners — including industry, government, and international research institutions — are encouraged, subject to the following conditions:

(a) **Ethical alignment.** External partners shall be willing to comply with this policy's ethical standards and with Nigerian law.

(b) **Data protection.** Data sharing agreements shall comply with the NDPA and this policy's data governance provisions.

(c) **Intellectual property.** Intellectual property arrangements shall be documented in advance and shall be consistent with the University's Intellectual Property Policy.

(d) **Transparency.** The nature and extent of AI use in collaborative research shall be transparent to all partners and to the University's research governance bodies.

(e) **Capacity building.** Collaborations shall, where possible, contribute to building AI research capacity at McPherson University.

13.7 Commercialisation and Technology Transfer

AI-related research at McPherson University may result in commercially valuable intellectual property. The University's existing Intellectual Property Policy and Commercialisation Framework shall govern the commercialisation of AI-related research outputs. Researchers shall:

(a) Disclose AI-related inventions and works to the Research Office in accordance with University procedures;

(b) Comply with the University's intellectual property and revenue-sharing policies;

(c) Consider the ethical implications of commercialising AI technologies, particularly where such technologies may have dual-use or harmful applications;

(d) Ensure that commercialisation activities are consistent with the University's mission and values.

Section 14: Postgraduate Research and AI

14.1 AI Use in Thesis and Dissertation Work

Postgraduate research at McPherson University — including PGD, M.Sc., MPhil, and Ph.D. programmes — is subject to the same AI governance principles as other research, with additional requirements appropriate to the advanced nature of the work.

Postgraduate students may use AI tools in their thesis or dissertation work in accordance with the categories and disclosure requirements established in this policy. The extent of permitted AI use shall be determined

by the supervisor in consultation with the student, having regard to the nature of the research, the requirements of the discipline, and the learning objectives of the programme.

Postgraduate theses and dissertations shall include an AI Use Disclosure Statement specifying:

- (a) The AI tools used;
- (b) The purposes for which AI was used;
- (c) The extent to which AI contributed to the work;
- (d) How AI-generated content was verified;
- (e) A declaration that the student takes full responsibility for the accuracy and integrity of the final submission.

14.2 Supervisor Responsibilities

Postgraduate supervisors at McPherson University have specific responsibilities in relation to AI use by their students:

- (a) **Guidance.** Supervisors shall provide clear guidance to students on the permissible and impermissible uses of AI in their research, consistent with this policy and disciplinary standards.
- (b) **Oversight.** Supervisors shall maintain oversight of AI use in their students' research, including through regular discussions and review of draft materials.
- (c) **Verification.** Supervisors shall satisfy themselves that AI-generated content has been appropriately verified and that the student's intellectual contribution remains substantive.
- (d) **Disclosure review.** Supervisors shall review AI Use Disclosure Statements and ensure that they are accurate and complete before thesis submission.
- (e) **Reporting concerns.** Supervisors shall report any concerns about AI-related misconduct to the appropriate University authority.
- (f) **Modelling.** Supervisors shall model responsible AI use in their own research and professional practice.

14.3 Examination and Viva Voce Considerations

The examination of postgraduate theses at McPherson University shall take account of AI-related issues:

- (a) **Examiner guidance.** Examiners shall be provided with guidance on the University's AI policy and on identifying potential AI-related concerns in theses.
- (b) **Viva voce examination.** The viva voce examination provides an opportunity for examiners to probe the candidate's understanding of their work, including the role of AI and the candidate's own intellectual contribution.
- (c) **AI-related questions.** Examiners may ask candidates to explain their AI use, defend the accuracy of AI-assisted analysis, and demonstrate their independent understanding of the research.
- (d) **Verification of authorship.** Where AI-related concerns arise, examiners may require the candidate to demonstrate authorship through additional verification procedures.

(e) **Outcome determination.** AI-related concerns shall be considered in the determination of examination outcomes, in accordance with the University's examination regulations and academic misconduct procedures.

14.4 Research Integrity Training for Postgraduate Students

All postgraduate students at McPherson University shall receive research integrity training that includes AI-related content. This training shall cover:

- (a) The responsible use of AI in research;
- (b) Disclosure and attribution requirements;
- (c) Ethical issues in AI-assisted research;
- (d) Data protection and privacy in AI research;
- (e) The consequences of AI-related research misconduct.

Research integrity training shall be completed before the student commences substantive research work and shall be documented in the student's research progress records.

14.5 AI in Postgraduate Coursework

Postgraduate coursework — including taught modules, assignments, and examinations — shall be subject to the same AI use categories and disclosure requirements as undergraduate coursework, as detailed in Sections 8 and 9, with such adaptations as may be appropriate to the postgraduate context.

Postgraduate coursework in research methods shall include explicit attention to the responsible use of AI in research, including practical exercises in AI-assisted literature review, data analysis, and writing, with critical reflection on the limitations and ethical implications of AI use.

Part Five: AI in Administration and Operations

Section 15: Administrative Use of AI

15.1 Foundational Position

McPherson University recognises that artificial intelligence can significantly enhance the efficiency, accuracy, and responsiveness of its administrative operations. From routine correspondence and scheduling to complex data analysis and reporting, AI tools offer opportunities to reduce administrative burden, free staff time for higher-value activities, and improve service delivery to students and other stakeholders.

At the same time, the University affirms that administrative AI use must be governed by the same principles of human-centred governance, accountability, transparency, equity, and data protection that apply throughout this policy. Administrative convenience shall never justify the erosion of human judgment, the compromise of personal data, or the circumvention of established governance procedures.

The University's approach to administrative AI is therefore permissive but regulated. Staff are encouraged to explore AI tools that enhance their work, subject to the requirements set out in this Section and the related provisions in Sections 16 to 18.

15.2 Permitted Administrative Applications

Subject to the requirements of this policy and any applicable University procedures, the following administrative uses of AI are permitted:

- (a) **Correspondence and communication.** Using AI to draft, edit, or translate routine correspondence, memoranda, circulars, and other communications, provided the substantive content is reviewed and approved by the responsible officer.
- (b) **Scheduling and calendar management.** Using AI tools to assist with scheduling meetings, managing calendars, and coordinating events, provided final scheduling decisions remain subject to human confirmation.
- (c) **Document summarisation and analysis.** Using AI to summarise lengthy documents, extract key information, or identify patterns in administrative data, provided the accuracy of AI outputs is verified before reliance.
- (d) **Data analysis and reporting.** Using AI to assist with the analysis of administrative data, generation of reports, and preparation of statistical summaries, provided the methods and results are understood and can be explained by the responsible officer.
- (e) **Drafting and editing support.** Using AI for grammar checking, style improvement, formatting, and language editing of administrative documents, provided the substantive content and decisions remain the responsibility of the human author.
- (f) **Research and information gathering.** Using AI to locate relevant policies, regulations, precedents, or background information to support administrative decision-making, provided the reliability of AI outputs is independently verified.

(g) **Meeting and minute support.** Using AI tools to transcribe meetings or generate draft minutes, provided the accuracy of transcripts and minutes is verified and final approval rests with the appropriate officer or body.

(h) **Customer service and enquiry handling.** Using AI-powered chatbots or virtual assistants to handle routine enquiries, provided such systems are appropriately configured, monitored, and escalated to human staff where necessary.

15.3 Prohibited Administrative Applications

The following administrative uses of AI are prohibited:

(a) **Autonomous decision-making.** Using AI to make decisions that affect the rights, privileges, or obligations of students, staff, or other persons without meaningful human review and approval.

(b) **Processing of sensitive personal data without safeguards.** Using AI to process sensitive personal data (as defined in the NDPA) without appropriate data protection safeguards and, where required, a Data Privacy Impact Assessment.

(c) **Unauthorised access to restricted data.** Using AI tools to access, analyse, or process data that the staff member is not authorised to access.

(d) **Financial transactions without human approval.** Using AI to execute financial transactions, approve expenditures, or commit the University to contractual obligations without appropriate human authorisation.

(e) **Generating official University positions.** Using AI to generate statements, positions, or communications that purport to represent the official position of the University without appropriate authorisation.

(f) **Circumventing established procedures.** Using AI to bypass or circumvent established University procedures for procurement, approval, consultation, or record-keeping.

(g) **Use of unapproved AI tools for confidential data.** Using unapproved or unauthorised AI tools to process confidential University data, including student records, staff records, financial data, or research data.

(h) **Deceptive or misleading use.** Using AI to generate deceptive, misleading, or fraudulent content, including falsified records, communications, or reports.

15.4 Human Oversight Requirements for AI-Assisted Administrative Decisions

All administrative decisions assisted by AI shall be subject to meaningful human oversight. The responsible human officer shall:

(a) **Review AI outputs.** Review and evaluate AI-generated recommendations, analyses, or draft decisions before acting on them.

(b) **Exercise independent judgment.** Apply their own knowledge, experience, and professional judgment to the decision, rather than deferring uncritically to AI outputs.

(c) **Verify accuracy.** Verify the accuracy of AI-generated information, particularly where it relates to legal requirements, financial matters, or individual rights.

(d) **Document the decision.** Maintain appropriate records of the decision-making process, including the role played by AI and the basis for the final human decision.

(e) **Take responsibility.** Accept personal responsibility for the decision and its consequences, notwithstanding the involvement of AI.

Where an AI-assisted decision affects a student or staff member adversely, the affected person shall have the right to request human review of the decision, consistent with Section 19.7.

15.5 Procurement and Evaluation of AI Tools

The procurement of AI tools and services by McPherson University shall be subject to the following requirements:

(a) **Needs assessment.** Before procuring an AI tool, the requesting unit shall conduct a needs assessment that identifies the problem to be solved, the expected benefits, and alternative solutions (including non-AI solutions).

(b) **Privacy assessment.** Where the AI tool will process personal data, a Data Privacy Impact Assessment shall be conducted in accordance with Section 19.4.

(c) **Security assessment.** The ICT Directorate shall assess the security of the AI tool, including data storage, transmission, access controls, and vulnerability management.

(d) **Ethical assessment.** The requesting unit, in consultation with the AI Policy Committee, shall assess the AI tool for potential ethical concerns, including bias, equity impacts, and alignment with University values.

(e) **Cost-benefit analysis.** The requesting unit shall prepare a cost-benefit analysis that considers not only financial costs but also staff time, training requirements, integration effort, and ongoing maintenance.

(f) **Pilot testing.** Where appropriate, the AI tool shall be piloted in a limited context before full deployment, with evaluation of performance, usability, and risk.

(g) **Approval.** Procurement of AI tools shall be subject to the University's established procurement approval procedures, with additional review by the AI Policy Committee for tools that process personal data, affect individual rights, or involve significant expenditure.

15.6 Vendor and Third-Party AI Service Agreements

Contracts with third-party AI service providers shall include provisions addressing:

(a) **Data protection.** Compliance with the NDPA, including data processing agreements, data subject rights, and breach notification obligations.

(b) **Data ownership.** Clarification that the University retains ownership of its data and that vendors do not acquire rights to use University data for their own purposes without explicit consent.

(c) **Data location.** Disclosure of where University data will be stored and processed, and compliance with any applicable data localisation requirements.

(d) **Security.** Minimum security standards, including encryption, access controls, and incident response procedures.

(e) **Service levels.** Performance standards, uptime commitments, and support arrangements.

- (f) **Audit rights.** The University's right to audit vendor compliance with contractual requirements.
- (g) **Termination and data portability.** Procedures for termination, including return or deletion of University data and transition assistance.
- (h) **Liability.** Allocation of liability for data breaches, service failures, and other risks.

The University's Legal Unit and ICT Directorate shall review AI vendor agreements to ensure compliance with these requirements.

15.7 Integration with Existing University Systems

Where AI tools are integrated with existing University systems (such as the student records system, financial management system, or human resources system), the integration shall be subject to:

- (a) **Compatibility assessment.** Confirmation that the AI tool can integrate with existing systems without compromising functionality or security.
- (b) **Data flow mapping.** Documentation of how data will flow between systems, including any data sharing with external parties.
- (c) **Access controls.** Maintenance of appropriate access controls to ensure that AI tools do not create unauthorised access pathways.
- (d) **Change management.** Coordination with the ICT Directorate and affected units to manage the integration process and minimise disruption.
- (e) **Testing and validation.** Thorough testing of the integrated system before deployment, including testing for data accuracy, security, and performance.

15.8 Training for Administrative Staff

Administrative staff shall receive training on the responsible use of AI in their work. This training shall cover:

- (a) **Approved tools and applications.** Which AI tools are approved for use and for what purposes.
- (b) **Prohibited uses.** What administrative uses of AI are prohibited and why.
- (c) **Human oversight requirements.** How to review, verify, and take responsibility for AI-assisted decisions.
- (d) **Data protection.** How to handle personal data when using AI tools.
- (e) **Security awareness.** How to recognise and report AI-related security risks.
- (f) **Ethical considerations.** How to identify and address ethical concerns in administrative AI use.
- (g) **Reporting concerns.** How to report AI-related problems, incidents, or concerns.

Training shall be provided as part of staff induction and through periodic refresher sessions. The Human Resources Unit, in collaboration with the ICT Directorate and the AI Policy Committee, shall coordinate the delivery of this training.

Section 16: Student Records, Admissions, and Assessment Administration

16.1 AI in Admissions Processes

McPherson University may use AI tools to support admissions processes, subject to the following requirements:

- (a) **Human decision-making.** Final admission decisions shall be made by authorised human admissions officers. AI tools may be used to assist with application review, ranking, or screening, but shall not make autonomous admission decisions.
- (b) **Transparency.** Applicants shall be informed where AI tools are used in the admissions process and how they may request human review of any AI-assisted decision.
- (c) **Bias monitoring.** AI tools used in admissions shall be monitored for bias, particularly in relation to gender, ethnicity, religion, disability, and socio-economic background. The University shall take reasonable steps to mitigate identified bias.
- (d) **Data protection.** Personal data processed in AI-assisted admissions shall be handled in accordance with the NDPA and Section 19 of this policy.
- (e) **Equity.** The University shall ensure that AI-assisted admissions do not disadvantage applicants from underrepresented or underserved groups.

16.2 AI in Student Records Management

AI tools used in student records management shall comply with the following requirements:

- (a) **Accuracy.** AI-assisted records management shall maintain the accuracy and completeness of student records. Errors introduced by AI shall be identified and corrected promptly.
- (b) **Security.** Student records processed by AI tools shall be protected by appropriate security measures, including access controls and encryption.
- (c) **Confidentiality.** AI tools shall not disclose student records to unauthorised persons, whether within or outside the University.
- (d) **Retention.** AI-assisted records management shall comply with the University's records retention and disposal policies, and with any applicable legal requirements.
- (e) **Access rights.** Students' rights to access, review, and request correction of their records shall be preserved, regardless of AI involvement in records management.

16.3 AI in Academic Advising

AI tools may be used to support academic advising, subject to the following conditions:

- (a) **Human advisor relationship.** AI shall supplement, not replace, the relationship between students and their human academic advisors. Students shall retain access to human advisors for guidance, mentorship, and support.
- (b) **Accuracy.** AI-generated advice on course selection, programme requirements, or academic progress shall be verified against authoritative University records before being communicated to students.

(c) **Transparency.** Students shall be informed when AI tools are used in academic advising and shall be able to request human review of any AI-generated advice.

(d) **Limitations.** AI advising tools shall clearly communicate their limitations, particularly in relation to complex or individual circumstances that may require human judgment.

(e) **Privacy.** Personal data used in AI-assisted advising shall be protected in accordance with Section 19.

16.4 AI in Examination Administration

AI tools may be used in examination administration — including scheduling, invigilation support, and marking assistance — subject to the following requirements:

(a) **Human marking.** Final marks and grades shall be determined by human examiners. AI marking tools may be used to assist with preliminary marking, consistency checking, or feedback generation, but shall not determine final outcomes.

(b) **Quality assurance.** AI-assisted marking shall be subject to quality assurance procedures to ensure accuracy, consistency, and fairness.

(c) **Transparency.** Students shall be informed where AI tools are used in marking or examination administration, and shall be able to request human review of AI-assisted marking.

(d) **Appeals.** The University's examination appeals procedures shall apply to AI-assisted marking, and students shall have the right to human re-marking where they have grounds for appeal.

(e) **Security.** AI tools used in examination administration shall be secure from unauthorised access and manipulation.

16.5 Automated Decision-Making Restrictions Under NDPA

Section 37 of the Nigeria Data Protection Act 2023 provides that data subjects have the right not to be subjected to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects.

McPherson University shall comply with this requirement. In practice, this means that:

(a) **No solely automated decisions.** The University shall not make decisions about students, staff, or other data subjects that are based solely on automated processing and that produce legal or similarly significant effects.

(b) **Meaningful human involvement.** All such decisions shall involve meaningful human review and judgment. Human involvement shall not be merely nominal or tokenistic.

(c) **Information and rights.** Data subjects shall be informed when automated processing is used to support decisions and shall be informed of their right to request human intervention, express their point of view, and contest the decision.

(d) **Safeguards.** The University shall implement appropriate safeguards for automated processing, including regular reviews of AI systems, documentation of decision-making processes, and mechanisms for addressing errors or biases.

16.6 Right to Human Review of Automated Decisions

Where the University uses AI to support decisions that affect students or staff, the affected person shall have the right to:

- (a) **Request human review.** Request that the decision be reviewed by a human decision-maker with the authority to confirm, modify, or overturn the AI-assisted decision.
- (b) **Express their point of view.** Provide information or arguments that they believe should be considered in the review.
- (c) **Receive reasons.** Receive an explanation of the decision, including the role played by AI and the basis for the final human determination.
- (d) **Contest the decision.** Contest the decision through the University's established appeals or grievance procedures.
- (e) **Be informed.** Be informed of these rights when they are subject to an AI-assisted decision that affects them adversely.

16.7 Data Retention and Disposal

AI systems that process student or staff data shall comply with the University's data retention and disposal policies. This includes:

- (a) **Retention schedules.** Data shall be retained only for as long as necessary for the purposes for which it was collected, or as required by law.
- (b) **Secure disposal.** When data is no longer needed, it shall be securely disposed of in accordance with University procedures and the NDPA.
- (c) **AI system data.** Data held within AI systems (including training data, logs, and outputs) shall be subject to the same retention and disposal requirements as other University data.
- (d) **Vendor compliance.** Contracts with AI vendors shall include provisions for the secure disposal of University data upon termination or expiry of the contract.

Section 17: Finance, Procurement, and Resource Management

17.1 AI in Budgeting and Financial Planning

AI tools may be used to support budgeting and financial planning, subject to the following conditions:

- (a) **Human approval.** AI-generated budget proposals, forecasts, and financial analyses shall be reviewed and approved by authorised human officers before adoption.
- (b) **Accuracy verification.** AI-generated financial data and projections shall be verified against authoritative University financial records.
- (c) **Transparency.** The use of AI in budgeting and financial planning shall be documented, and the basis for financial decisions shall be clearly articulated.
- (d) **Confidentiality.** Financial data processed by AI tools shall be protected by appropriate security measures and shall not be disclosed to unauthorised persons.

17.2 AI in Procurement and Vendor Management

AI tools may be used to support procurement and vendor management, subject to the following conditions:

- (a) **Human decision-making.** Procurement decisions shall be made by authorised human officers. AI tools may assist with vendor evaluation, price comparison, and contract analysis, but shall not make autonomous procurement decisions.
- (b) **Fairness.** AI-assisted procurement shall not discriminate against vendors on the basis of protected characteristics or engage in anti-competitive practices.
- (c) **Transparency.** The use of AI in procurement shall be documented, and vendors shall be informed where AI tools are used in the evaluation of their bids.
- (d) **Conflicts of interest.** AI-assisted procurement shall be subject to the University's conflict of interest policies, and AI tools shall not be used to circumvent these policies.

17.3 Cost-Benefit Assessment for AI Investments

Proposals to invest in AI tools or infrastructure shall include a cost-benefit assessment that considers:

- (a) **Direct costs.** Purchase or subscription costs, implementation costs, training costs, and ongoing maintenance costs.
- (b) **Indirect costs.** Staff time, integration effort, change management, and potential productivity impacts.
- (c) **Expected benefits.** Efficiency gains, quality improvements, service enhancements, and strategic value.
- (d) **Risks.** Implementation risks, security risks, privacy risks, and ethical risks.
- (e) **Alternatives.** Non-AI alternatives and their comparative costs and benefits.
- (f) **Sustainability.** Long-term sustainability of the investment, including ongoing resource requirements.

17.4 Licensing and Subscription Management

The University shall maintain a register of AI tools and services licensed or subscribed to by the University. This register shall include:

- (a) The name and description of the AI tool or service;
- (b) The unit or units using the tool;
- (c) The licensing or subscription terms, including costs and renewal dates;
- (d) The categories of data processed by the tool;
- (e) The responsible officer for the tool;
- (f) Any applicable data processing agreements or security assessments.

The ICT Directorate shall maintain this register in collaboration with the Procurement Unit and the AI Policy Committee.

17.5 Sustainability Considerations

When evaluating AI investments, the University shall consider sustainability factors, including:

- (a) **Environmental impact.** The energy consumption and carbon footprint of AI systems, particularly for computationally intensive applications.
- (b) **Financial sustainability.** The ongoing costs of AI tools and infrastructure, and their alignment with the University's financial capacity.
- (c) **Institutional sustainability.** The alignment of AI investments with the University's strategic priorities and mission.
- (d) **Capacity sustainability.** The availability of staff with the skills to manage and maintain AI systems.

Section 18: Human Resources and Staff Management

18.1 AI in Recruitment and Selection

McPherson University may use AI tools to support recruitment and selection, subject to the following requirements:

- (a) **Human decision-making.** Final recruitment and selection decisions shall be made by authorised human officers. AI tools may assist with candidate screening, CV analysis, or interview scheduling, but shall not make autonomous hiring decisions.
- (b) **Transparency.** Candidates shall be informed where AI tools are used in the recruitment process and shall be able to request human review of any AI-assisted decision.
- (c) **Bias monitoring.** AI tools used in recruitment shall be monitored for bias, particularly in relation to gender, ethnicity, religion, disability, and age. The University shall take reasonable steps to mitigate identified bias.
- (d) **Data protection.** Personal data processed in AI-assisted recruitment shall be handled in accordance with the NDPA and Section 19 of this policy.
- (e) **Equity.** The University shall ensure that AI-assisted recruitment does not disadvantage candidates from underrepresented groups.

18.2 AI in Performance Management

AI tools may be used to support performance management, subject to the following conditions:

- (a) **Human judgment.** Performance assessments and decisions shall be made by human supervisors. AI tools may provide data, analysis, or recommendations, but shall not determine performance outcomes.
- (b) **Transparency.** Staff shall be informed where AI tools are used in performance management and shall be able to discuss AI-generated assessments with their supervisors.
- (c) **Fairness.** AI-assisted performance management shall be fair, consistent, and free from discrimination.
- (d) **Context.** AI-generated performance data shall be interpreted in context, taking account of individual circumstances and the nature of the work.
- (e) **Appeals.** Staff shall have the right to appeal AI-assisted performance decisions through the University's established grievance procedures.

18.3 AI in Staff Development and Training

AI tools may be used to support staff development and training, including:

- (a) **Personalised learning.** AI-powered learning platforms that adapt to individual staff needs and preferences.
- (b) **Skills assessment.** AI tools that assess staff skills and identify development needs.
- (c) **Training delivery.** AI-assisted training content and delivery mechanisms.
- (d) **Career development.** AI tools that suggest career pathways and development opportunities.

Such uses shall comply with the data protection requirements in Section 19 and shall be subject to human oversight.

18.4 Protection of Staff Data

Staff personal data processed by AI tools shall be protected in accordance with the NDPA and Section 19 of this policy. This includes:

- (a) **Lawful processing.** Staff data shall be processed lawfully, fairly, and transparently.
- (b) **Purpose limitation.** Staff data shall be processed only for specified, explicit, and legitimate purposes.
- (c) **Data minimisation.** Only data necessary for the relevant purpose shall be processed.
- (d) **Accuracy.** Staff data shall be accurate and kept up to date.
- (e) **Security.** Staff data shall be protected by appropriate security measures.
- (f) **Rights.** Staff shall retain their rights under the NDPA, including rights of access, rectification, erasure, and objection.

18.5 AI-Related Job Displacement and Reskilling

The University recognises that AI adoption may lead to changes in job roles and, in some cases, job displacement. The University commits to:

- (a) **Transparent communication.** Keeping staff informed about AI adoption plans and their potential impacts on roles and responsibilities.
- (b) **Reskilling opportunities.** Providing training and development opportunities to help staff adapt to AI-augmented work environments.
- (c) **Redeployment.** Where possible, redeploying affected staff to alternative roles within the University.
- (d) **Fair treatment.** Ensuring that AI-related workforce changes are managed fairly, transparently, and in accordance with the University's human resources policies and applicable labour law.
- (e) **Consultation.** Consulting with staff and their representatives on AI adoption plans that may affect employment.

18.6 Staff Rights in AI-Augmented Workplaces

Staff at McPherson University shall retain the following rights in relation to AI in the workplace:

- (a) **Right to information.** The right to be informed about AI tools that affect their work or working conditions.
- (b) **Right to human review.** The right to request human review of AI-assisted decisions that affect them adversely.
- (c) **Right to privacy.** The right to privacy in relation to their personal data, in accordance with the NDPA and Section 19.
- (d) **Right to object.** The right to object to AI processing of their personal data in circumstances permitted by law.
- (e) **Right to dignity.** The right to be treated with dignity and respect, including in AI-augmented work environments.
- (f) **Right to development.** The right to access training and development opportunities to maintain and enhance their AI-related competencies.

Part Six: Data Governance and Privacy

Section 19: Data Protection Framework

19.1 Foundational Position

McPherson University affirms that the protection of personal data is both a legal obligation and a moral imperative. As an institution founded on Godly virtues and committed to integrity in all its operations, the University treats the personal data of its students, staff, and other stakeholders as a sacred trust. The University's approach to AI governance must therefore be grounded in robust data protection practices that comply fully with the Nigeria Data Protection Act 2023 (NDPA) and its General Application and Implementation Directive 2025 (GAID).

The University notes that the NDPA and GAID have established a comprehensive statutory regime for data protection in Nigeria, replacing the Nigeria Data Protection Regulation 2019. The NUC has emphasised that strengthening institutional data governance is a core component of its AI Policy Framework for the Nigerian University System, and the University aligns fully with this expectation. This Section establishes the data protection framework within which all AI-related processing of personal data at McPherson University shall occur.

19.2 Compliance with the Nigeria Data Protection Act 2023

McPherson University shall comply fully with the NDPA, which applies to all processing of personal data by the University as a data controller. The University's obligations under the NDPA include:

- (a) **Lawful processing.** All personal data processed by AI systems shall be processed lawfully, fairly, and transparently, in accordance with a valid lawful basis under Section 25 of the NDPA.
- (b) **Purpose limitation.** Personal data shall be collected for specified, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes.
- (c) **Data minimisation.** AI systems shall process only the personal data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- (d) **Accuracy.** Personal data processed by AI systems shall be accurate and, where necessary, kept up to date. AI systems shall include mechanisms for identifying and correcting inaccuracies.
- (e) **Storage limitation.** Personal data shall be retained only for as long as necessary for the purposes for which it is processed, in accordance with the University's records retention policy.
- (f) **Integrity and confidentiality.** AI systems shall implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage.
- (g) **Accountability.** The University shall be able to demonstrate compliance with these principles, including through documentation, audits, and the designation of a Data Protection Officer.

19.3 Lawful Bases for Processing Personal Data

The University shall ensure that all AI-related processing of personal data is grounded in a valid lawful basis. Permissible lawful bases under the NDPA include:

- (a) **Consent.** The data subject has given consent to the processing of their personal data for one or more specific purposes. Where consent is the lawful basis, the University shall ensure that consent is freely given, specific, informed, and unambiguous, and shall maintain records of consent.
- (b) **Contract.** Processing is necessary for the performance of a contract to which the data subject is a party, or for taking steps at the request of the data subject prior to entering into a contract.
- (c) **Legal obligation.** Processing is necessary for compliance with a legal obligation to which the University is subject.
- (d) **Vital interests.** Processing is necessary to protect the vital interests of the data subject or another person.
- (e) **Public interest.** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the University.
- (f) **Legitimate interests.** Processing is necessary for the purposes of legitimate interests pursued by the University or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

The GAID introduces specific requirements for relying on legitimate interest as a lawful basis, including the conduct of a Legitimate Interest Assessment. The University shall comply with these requirements where legitimate interest is relied upon.

19.4 Data Protection Officer Designation and Responsibilities

In accordance with Section 32 of the NDPA and the GAID, McPherson University shall designate a Data Protection Officer (DPO) with the authority and resources to ensure compliance with the NDPA and this policy.

The DPO shall:

- (a) **Advise on compliance.** Provide expert advice to the University on its obligations under the NDPA and other applicable data protection laws, particularly in relation to AI systems.
- (b) **Monitor compliance.** Monitor the University's compliance with the NDPA, the GAID, and this policy, including through audits, assessments, and reviews.
- (c) **Serve as contact point.** Serve as the primary contact point for data subjects exercising their rights under the NDPA and for the Nigeria Data Protection Commission.
- (d) **Conduct Data Privacy Impact Assessments.** Coordinate and review Data Privacy Impact Assessments for AI systems that process personal data.
- (e) **Prepare compliance reports.** Prepare and submit the semi-annual data protection report required under the GAID, detailing the University's compliance status.
- (f) **Deliver training and awareness.** Lead data protection training and awareness initiatives across the University, including in relation to AI.
- (g) **Maintain records.** Maintain records of processing activities, data breaches, and other compliance documentation.

The University notes that the NDPC has issued compliance notices to 649 Nigerian tertiary institutions requiring, among other things, proof of appointment of a Data Protection Officer and evidence of Data

Protection Compliance Audit Returns filing. The University shall ensure full compliance with these requirements.

19.5 Data Privacy Impact Assessments for AI Systems

The University shall conduct a Data Privacy Impact Assessment (DPIA) before deploying any AI system that processes personal data and is likely to result in a high risk to the rights and freedoms of data subjects. This requirement is mandated by the NDPA and further detailed in the GAID, which provides a standardised template for conducting DPIAs.

A DPIA shall include:

- (a) **Description of the processing.** A systematic description of the AI system, the personal data it processes, the purposes of processing, and the legitimate interest pursued (where applicable).
- (b) **Necessity and proportionality assessment.** An assessment of whether the processing is necessary and proportionate to the purposes for which it is intended.
- (c) **Risk assessment.** An assessment of the risks to the rights and freedoms of data subjects arising from the processing, including risks of discrimination, bias, and algorithmic harm.
- (d) **Mitigation measures.** A description of the measures envisaged to address the identified risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data.
- (e) **Consultation.** Where appropriate, consultation with the DPO and, where required, with the NDPC.
- (f) **Review and documentation.** Regular review of the DPIA to ensure that it remains accurate and up to date.

The DPO shall maintain a register of all DPIAs conducted and shall report on their status to the AI Policy Committee and the Senate as required.

19.6 Consent Requirements for AI Processing

Where consent is the lawful basis for AI processing of personal data, the University shall ensure that:

- (a) **Consent is freely given.** Consent shall not be obtained through coercion, undue influence, or as a condition of enrolment, employment, or service provision.
- (b) **Consent is specific.** Consent shall be obtained for specific purposes and shall not be construed as blanket authorisation for all AI processing.
- (c) **Consent is informed.** Data subjects shall be provided with clear, accessible information about the AI processing, including its purposes, the categories of data involved, and the rights available to them.
- (d) **Consent is unambiguous.** Consent shall be expressed through a clear affirmative action and shall not be inferred from silence or inactivity.
- (e) **Consent is documented.** The University shall maintain records of consent, including when, how, and for what purposes consent was given.
- (f) **Consent is withdrawable.** Data subjects shall be able to withdraw consent at any time, without detriment, and the University shall provide accessible mechanisms for withdrawal.

The GAID explicitly provides that consent is required before a data controller makes a decision based solely on automated processing which produces legal effects concerning or significantly affecting the data subject.

19.7 Data Subject Rights

The University shall facilitate the exercise of data subject rights under the NDPA. These rights include:

- (a) **Right to information.** Data subjects have the right to be informed about the collection and use of their personal data, including in AI systems.
- (b) **Right of access.** Data subjects have the right to access their personal data and to obtain information about how it is processed.
- (c) **Right to rectification.** Data subjects have the right to request the correction of inaccurate or incomplete personal data.
- (d) **Right to erasure.** Data subjects have the right to request the deletion of their personal data in certain circumstances.
- (e) **Right to restriction.** Data subjects have the right to request the restriction of processing of their personal data in certain circumstances.
- (f) **Right to data portability.** Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format.
- (g) **Right to object.** Data subjects have the right to object to the processing of their personal data in certain circumstances.
- (h) **Rights related to automated decision-making.** Data subjects have the right not to be subjected to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects, as detailed in Section 19.8.

The DPO shall establish accessible procedures for data subjects to exercise these rights, and the University shall respond to requests within the timeframes established by the NDPA.

19.8 Automated Decision-Making Restrictions Under NDPA Section 37

Section 37 of the NDPA guarantees data subjects the right not to be subjected to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects. The University shall comply fully with this requirement.

To determine whether Section 37 is engaged, the University shall apply a three-part cumulative test:

- (a) **A decision.** There must be a definitive outcome or determination regarding a data subject.
- (b) **Solely automated basis.** The processing must be conducted without meaningful human oversight or evaluation of personal data.
- (c) **Legal or similarly significant effects.** The decision must alter an individual's legal status, rights, or materially impact their financial, contractual, or personal position.

Where any of these elements is absent, Section 37 is not engaged. However, where all three elements are present, the University shall ensure that one of the statutory exceptions applies:

(a) **Contract necessity.** The decision is necessary for entering into or performing a contract between the data subject and the University.

(b) **Legal authorisation.** The decision is authorised by written law applicable to the University, and that law provides appropriate safeguards for the data subject's rights and interests.

(c) **Explicit consent.** The decision is based on the data subject's explicit consent.

Even where an exception applies, the University shall ensure that data subjects have the right to seek human intervention, express their point of view, and contest the decision. The University shall also provide meaningful information about the logic involved, as well as the significance and envisaged consequences of the processing.

The University notes the emerging jurisprudence suggesting that where a data controller deploys automated decision-making systems, the evidentiary burden may shift to the controller to demonstrate the system's legality, accuracy, and non-discriminatory nature. The University shall therefore maintain comprehensive documentation of all automated decision-making systems, including their logic, error rates, and known limitations.

19.9 Cross-Border Data Transfer Rules

The University acknowledges that many AI tools and services involve the transfer of personal data outside Nigeria. Under the NDPA and GAID, cross-border data transfers are permitted only where:

(a) **Adequacy.** The recipient country or international organisation ensures an adequate level of protection for personal data, as determined by an adequacy decision of the Nigeria Data Protection Commission.

(b) **Appropriate safeguards.** The University and the recipient have entered into a Cross-Border Data Transfer Instrument (CBDTI) approved by the Commission, or other appropriate safeguards are in place.

(c) **Derogations.** One of the derogations in Section 43 of the NDPA applies, including explicit consent, contract necessity, important reasons of public interest, or the establishment, exercise, or defence of legal claims.

Before transferring personal data to any AI service provider outside Nigeria, the University shall:

(a) Assess the adequacy of the recipient's data protection regime;

(b) Ensure that appropriate contractual safeguards are in place;

(c) Inform data subjects of the transfer and the risks involved;

(d) Obtain explicit consent where required; and

(e) Document the legal basis for the transfer.

The DPO shall maintain a register of all cross-border data transfers involving personal data.

19.10 Data Breach Notification and Response

The University shall implement procedures for detecting, investigating, and responding to personal data breaches involving AI systems. These procedures shall comply with the NDPA's breach notification requirements, which require notification to the Nigeria Data Protection Commission within 72 hours of

becoming aware of a breach, and notification to affected data subjects where the breach is likely to result in a high risk to their rights and freedoms.

The University's breach response procedures shall include:

- (a) **Detection and reporting.** Mechanisms for detecting and reporting suspected data breaches.
- (b) **Investigation.** Prompt investigation of reported breaches to determine their scope, cause, and impact.
- (c) **Containment.** Measures to contain the breach and prevent further unauthorised access or disclosure.
- (d) **Notification.** Notification to the NDPC and affected data subjects as required by law.
- (e) **Remediation.** Measures to address the cause of the breach and prevent recurrence.
- (f) **Documentation.** Records of all breaches, including their facts, effects, and remedial actions taken.

The DPO shall lead the University's breach response, in coordination with the ICT Directorate and the AI Policy Committee.

Section 20: Institutional Data Governance for AI

20.1 Data Governance Framework

McPherson University shall establish and maintain a comprehensive data governance framework for AI that addresses the classification, ownership, quality, security, and lifecycle management of data used in AI systems. This framework shall be overseen by the AI Policy Committee in collaboration with the ICT Directorate and the DPO.

20.2 Classification of University Data

The University shall classify its data according to sensitivity and criticality, and shall apply appropriate controls to each category. The classification scheme shall include:

- (a) **Public data.** Data that is freely available to the public, such as published research outputs, institutional statistics, and public communications.
- (b) **Internal data.** Data intended for use within the University, such as internal memoranda, operational procedures, and non-sensitive administrative records.
- (c) **Confidential data.** Data that requires protection from unauthorised disclosure, such as student records, staff records, financial data, and research data not yet published.
- (d) **Sensitive data.** Data that is subject to enhanced protection under the NDPA, including sensitive personal data as defined in the Act (data revealing racial or ethnic origin, political opinions, religious beliefs, health status, sexual orientation, and biometric data).
- (e) **Restricted data.** Data that is subject to the highest level of protection, including examination papers, security information, and data protected by legal privilege.

AI systems shall not process confidential, sensitive, or restricted data without appropriate safeguards and, where required, a DPIA.

20.3 Ownership and Stewardship of Institutional Data

The University affirms that institutional data is a University asset. The following principles shall apply:

- (a) **Ownership.** The University owns the data generated, collected, or maintained in the course of its operations, subject to applicable legal and contractual obligations.
- (b) **Stewardship.** Each unit of the University is responsible for the stewardship of data within its domain, including ensuring data quality, security, and compliance with this policy.
- (c) **Individual rights.** Individuals retain rights over their personal data as provided under the NDPA.
- (d) **Data sharing.** Data sharing within the University shall be governed by this policy and any applicable data sharing agreements.
- (e) **External sharing.** Data sharing with external parties shall be governed by written agreements that address data protection, ownership, use, and security.

20.4 Data Quality Standards for AI Training and Operation

The University shall establish and maintain data quality standards for AI systems. These standards shall address:

- (a) **Accuracy.** Data used in AI systems shall be accurate, complete, and up to date.
- (b) **Relevance.** Data shall be relevant to the purposes for which the AI system is used.
- (c) **Representativeness.** Data used for training AI systems shall be representative of the populations and contexts to which the AI system will be applied.
- (d) **Bias assessment.** Data shall be assessed for bias, and appropriate measures shall be taken to mitigate bias before use in AI systems.
- (e) **Provenance.** The source and lineage of data used in AI systems shall be documented.
- (f) **Validation.** Data quality shall be validated before use and periodically thereafter.

20.5 Prohibition on Using Institutional Data for Unauthorised AI Training

The University prohibits the use of institutional data for the training, fine-tuning, or development of AI models without explicit authorisation from the appropriate University authority. This prohibition applies to:

- (a) **External AI services.** University data shall not be uploaded to external AI services where the service provider's terms permit the use of such data for training or improving their models, unless explicitly authorised and appropriate safeguards are in place.
- (b) **Internal AI development.** University data shall not be used for internal AI development projects without approval from the AI Policy Committee and compliance with this policy.
- (c) **Student and staff data.** Personal data of students and staff shall not be used for AI training without a valid lawful basis and appropriate safeguards.

20.6 Data Minimisation and Purpose Limitation

AI systems deployed by the University shall comply with the principles of data minimisation and purpose limitation. Specifically:

- (a) **Minimal data collection.** AI systems shall collect only the data necessary for the specified purpose.

(b) **Purpose specificity.** Data collected for one purpose shall not be used for another purpose without a valid lawful basis and appropriate transparency.

(c) **Retention limitation.** Data shall not be retained beyond the period necessary for the specified purpose.

(d) **Anonymisation and pseudonymisation.** Where possible, data used in AI systems shall be anonymised or pseudonymised to reduce privacy risks.

20.7 Audit Trails and Logging for AI Systems

The University shall maintain audit trails and logs for AI systems that process personal data or support significant decisions. These logs shall include:

(a) **Data access logs.** Records of who accessed what data and when.

(b) **Processing logs.** Records of AI processing activities, including inputs, outputs, and decisions.

(c) **Model logs.** Records of AI model versions, updates, and changes.

(d) **Decision logs.** Records of decisions supported by AI, including the human review process.

(e) **Incident logs.** Records of AI-related incidents, including errors, breaches, and complaints.

Audit logs shall be retained for a period determined by the University's records retention policy, and shall be accessible to the DPO, the AI Policy Committee, and internal auditors as required.

20.8 Data Retention and Disposal Schedules

The University shall establish and maintain data retention and disposal schedules for data processed by AI systems. These schedules shall:

(a) Specify the retention period for each category of data;

(b) Identify the legal or operational basis for the retention period;

(c) Establish procedures for secure disposal of data at the end of the retention period;

(d) Ensure compliance with the NDPA's storage limitation principle; and

(e) Address the retention and disposal of data held within AI systems, including training data, logs, and outputs.

Section 21: Privacy of Student and Staff Data

21.1 Protection of Student Academic Records

Student academic records are among the most sensitive data held by the University. AI systems that process student records shall comply with the following requirements:

(a) **Confidentiality.** Student records shall not be disclosed to unauthorised persons, whether through AI systems or otherwise.

(b) **Access controls.** AI systems that process student records shall implement appropriate access controls to ensure that only authorised personnel can access such data.

(c) **Accuracy.** AI systems shall not introduce errors into student records. Any errors introduced by AI shall be identified and corrected promptly.

(d) **Student rights.** Students shall retain their rights under the NDPA, including rights of access, rectification, and objection.

(e) **Retention.** Student records shall be retained in accordance with the University's records retention policy.

21.2 Protection of Staff Personnel Records

Staff personnel records shall be protected in accordance with the NDPA and this policy. AI systems that process staff records shall:

(a) **Ensure confidentiality.** Staff records shall not be disclosed to unauthorised persons.

(b) **Implement access controls.** Only authorised personnel shall have access to staff records.

(c) **Maintain accuracy.** AI systems shall not introduce errors into staff records.

(d) **Respect staff rights.** Staff shall retain their rights under the NDPA.

(e) **Comply with retention requirements.** Staff records shall be retained in accordance with applicable law and University policy.

21.3 Protection of Health and Counselling Data

Health and counselling data are classified as sensitive personal data under the NDPA and require enhanced protection. AI systems that process such data shall:

(a) **Obtain explicit consent.** Processing of health and counselling data by AI systems shall be based on the explicit consent of the data subject, unless another lawful basis applies.

(b) **Implement enhanced security.** Health and counselling data shall be protected by encryption and other enhanced security measures.

(c) **Restrict access.** Access to health and counselling data shall be restricted to authorised health and counselling personnel.

(d) **Conduct DPIAs.** A DPIA shall be conducted before deploying any AI system that processes health or counselling data.

(e) **Prohibit unauthorised use.** Health and counselling data shall not be used for AI training or development without explicit authorisation and appropriate safeguards.

21.4 Protection of Research Participant Data

Research participant data shall be protected in accordance with the NDPA, the University's Research Ethics Policy, and any applicable ethical approvals. AI systems that process research participant data shall:

(a) **Comply with ethical approvals.** Processing shall be consistent with the terms of the ethical approval granted by the Research Ethics Committee.

(b) **Protect participant privacy.** Research participant data shall be anonymised or pseudonymised where possible.

(c) **Obtain consent.** Where required, informed consent shall be obtained from research participants for AI-related processing of their data.

(d) **Ensure security.** Research participant data shall be protected by appropriate security measures.

(e) **Respect withdrawal rights.** Research participants shall retain the right to withdraw their data from AI systems where feasible.

21.5 Prohibition on Unauthorised AI Profiling

The University prohibits the use of AI systems to profile students, staff, or other individuals for purposes that are not authorised by this policy or by law. Unauthorised profiling includes:

- (a) **Behavioural profiling.** Using AI to monitor and analyse individual behaviour without a valid lawful basis.
- (b) **Predictive profiling.** Using AI to predict individual characteristics, behaviour, or outcomes without appropriate safeguards.
- (c) **Discriminatory profiling.** Using AI to profile individuals based on protected characteristics in ways that result in discrimination.
- (d) **Covert profiling.** Using AI to profile individuals without their knowledge or consent where consent is required.

21.6 Transparency Regarding AI Processing of Personal Data

The University shall be transparent about its use of AI to process personal data. This includes:

- (a) **Privacy notices.** The University's privacy notices shall inform data subjects about the use of AI in processing their personal data.
- (b) **Specific notifications.** Where AI is used to make or support decisions that significantly affect individuals, those individuals shall be informed.
- (c) **Explanation of AI use.** The University shall provide meaningful information about the logic involved in AI processing, as well as the significance and envisaged consequences of such processing.
- (d) **Contact information.** Data subjects shall be provided with contact information for the DPO and for making enquiries or complaints about AI processing.

The University shall publish a summary of its AI systems that process personal data, including their purposes and categories of data processed, in a manner that is accessible to the University community.

Part Seven: Infrastructure, Security, and Risk Management

Section 22: ICT Infrastructure and AI Readiness

22.1 Foundational Position

McPherson University recognises that the responsible adoption of Artificial Intelligence is contingent upon the adequacy, reliability, and security of its underlying ICT infrastructure. The NUC's Artificial Intelligence Policy Framework and Implementation Roadmap has identified the harmonisation of compute infrastructure as a key priority for the Nigerian University System, and the NAAIP symposium of July 2026 underscored the need for investment in high-compute infrastructure and faculty training across Nigerian tertiary institutions. McPherson University aligns with this national direction and commits to the progressive strengthening of its ICT infrastructure to support AI-related teaching, learning, research, and administration.

The University affirms that infrastructure development for AI shall be guided by three principles: **adequacy** (the infrastructure must be sufficient for the University's current and projected AI needs); **reliability** (the infrastructure must perform consistently and securely); and **equity** (the infrastructure must be accessible to all members of the University community, without creating new digital divides).

22.2 Assessment of Current ICT Capacity for AI

The University shall conduct a comprehensive assessment of its current ICT capacity to support AI applications. This assessment shall address:

- (a) **Computing resources.** The availability of servers, workstations, and other computing resources capable of running AI applications, including GPU-enabled infrastructure where required for AI research and teaching.
- (b) **Network infrastructure.** The capacity, reliability, and coverage of the University's network infrastructure, including wired and wireless connectivity across lecture halls, laboratories, offices, hostels, and other campus locations.
- (c) **Internet bandwidth.** The adequacy of the University's internet bandwidth to support AI-related activities, including cloud-based AI services, data transfers, and collaborative research.
- (d) **Storage capacity.** The availability of adequate and secure data storage for AI-related data, models, and outputs.
- (e) **Software and platforms.** The availability of licensed and approved AI software, platforms, and development environments.
- (f) **Power supply.** The reliability of the University's power supply, including backup and alternative power arrangements to ensure continuous operation of AI-critical systems.

The ICT Directorate shall conduct this assessment within six months of the effective date of this policy and shall report its findings to the AI Policy Committee and the Senate.

22.3 Internet Connectivity and Bandwidth Requirements

The University shall ensure that internet connectivity is sufficient to support AI-related activities across all Colleges and units. The University notes the recent visit by MTN's technical crew to upgrade

telecommunications facilities on campus, which is expected to improve internet access, call quality, and overall network coverage across lecture halls, hostels, offices, and other areas on campus. The University shall build on this development to further enhance connectivity for AI-related activities.

Specific requirements shall include:

- (a) **Minimum bandwidth standards.** The University shall establish minimum bandwidth standards for different categories of AI-related activities, including teaching, research, and administration.
- (b) **Priority access.** Where necessary, the University shall implement priority access arrangements for AI-critical applications, ensuring that research and teaching activities are not compromised by non-essential network traffic.
- (c) **Redundancy.** The University shall maintain redundancy in its internet connectivity arrangements to ensure continuous access to AI services.
- (d) **Monitoring.** The ICT Directorate shall monitor network performance and shall report regularly to the AI Policy Committee on the adequacy of internet connectivity for AI-related activities.

22.4 Computing Resources for AI Research and Teaching

The University shall progressively develop computing resources to support AI research and teaching. This shall include:

- (a) **GPU-enabled workstations.** The University shall acquire GPU-enabled workstations and servers to support AI model training, data analysis, and computational research.
- (b) **Shared computing facilities.** Where individual acquisition is not feasible, the University shall establish shared computing facilities accessible to staff and students engaged in AI-related work.
- (c) **Cloud computing arrangements.** The University shall establish arrangements with reputable cloud service providers to supplement on-premises computing resources, subject to the data protection requirements in Section 19.
- (d) **Partnerships.** The University shall explore partnerships with other institutions, industry, and government agencies to access high-compute resources, including the regional high-compute hubs proposed by the NBTE at the NAAIP symposium.
- (e) **Resource allocation.** The University shall establish transparent procedures for allocating computing resources to research projects and teaching activities, prioritising projects that align with the University's mission and research priorities.

22.5 Cloud Services and Storage

The use of cloud services for AI-related activities shall be subject to the following requirements:

- (a) **Approved providers.** Cloud services shall be procured from providers that meet the University's security, privacy, and reliability standards.
- (b) **Data classification.** Data stored or processed in the cloud shall be classified in accordance with Section 20.2, and appropriate controls shall be applied based on data sensitivity.
- (c) **Data location.** The University shall ensure that cloud providers comply with the data localisation requirements of the NDPA and the GAID, where applicable.

(d) **Data processing agreements.** Contracts with cloud providers shall include data processing agreements that address the requirements of Section 15.6.

(e) **Exit strategy.** The University shall maintain an exit strategy for cloud services, including procedures for data return or deletion upon termination.

22.6 Power Reliability and Business Continuity

The University acknowledges that reliable power supply is a precondition for effective AI deployment. The University shall:

(a) **Assess power requirements.** Assess the power requirements of AI-related infrastructure, including computing resources, networking equipment, and cooling systems.

(b) **Ensure backup power.** Maintain backup power arrangements (such as generators and uninterruptible power supplies) sufficient to ensure continuity of AI-critical operations during power outages.

(c) **Monitor power quality.** Monitor power quality to protect sensitive AI equipment from damage.

(d) **Develop business continuity plans.** Develop and maintain business continuity and disaster recovery plans for AI systems, including procedures for restoring services after disruptions.

(e) **Explore sustainable solutions.** Explore sustainable power solutions, including solar and other renewable energy sources, to reduce dependence on unreliable grid power and to align with the University's environmental responsibilities.

22.7 Accessibility of AI Tools for All Students and Staff

The University affirms that access to AI tools shall not be a source of inequity within the University community. The University shall:

(a) **Provide institutional access.** Where AI tools are required or recommended for teaching or research, the University shall provide institutional access through site licences, shared accounts, or campus facilities.

(b) **Address the digital divide.** Recognise that students and staff have unequal access to personal devices, internet connectivity, and AI subscriptions, and shall take reasonable steps to mitigate these disparities.

(c) **Establish campus facilities.** Maintain campus facilities (such as computer laboratories and library workstations) equipped with AI tools accessible to students and staff who lack personal access.

(d) **Provide alternatives.** Where AI tools cannot be provided equitably, the University shall provide alternative arrangements that do not disadvantage any student or staff member.

(e) **Monitor accessibility.** Regularly monitor accessibility of AI tools and shall report to the AI Policy Committee on any barriers identified and measures taken to address them.

22.8 Infrastructure Development Roadmap

The University shall develop and maintain an Infrastructure Development Roadmap for AI that sets out:

(a) **Short-term priorities (0–12 months).** Assessment of current capacity, immediate upgrades to connectivity and power, and provision of foundational AI tools and facilities.

(b) **Medium-term priorities (1–3 years).** Development of computing resources, establishment of shared facilities, and expansion of cloud arrangements.

(c) **Long-term priorities (3–5 years).** Development of high-compute capabilities, exploration of partnerships for shared infrastructure, and integration of sustainable power solutions.

The Roadmap shall be reviewed annually by the AI Policy Committee and shall be aligned with the University's broader ICT strategy and strategic plan.

Section 23: Cybersecurity and AI

23.1 Foundational Position

McPherson University recognises that Artificial Intelligence introduces new dimensions to cybersecurity risk. AI systems can be targets of cyberattacks, instruments of cyberattacks, and amplifiers of existing vulnerabilities. The University notes that Nigerian universities have faced increasing cybersecurity threats, including deepfakes, phishing, and vishing attacks targeting institutions, and that experts have called for cybersecurity to be treated as a national priority through coordinated policies and stronger institutional responses. The University further notes the requirements of the Cybercrimes (Amendment) Act 2024, which establishes the legal framework for combating cybercrime in Nigeria.

The University shall implement appropriate technical and organisational measures to protect AI systems from unauthorised access, manipulation, or disruption, and shall prohibit the use of AI for malicious purposes. These measures shall be proportionate to the risks associated with different categories of AI use.

23.2 AI-Related Cybersecurity Risks

The University shall maintain awareness of AI-related cybersecurity risks, including:

- (a) **Adversarial attacks.** Manipulation of AI inputs to cause incorrect outputs or system failures.
- (b) **Data poisoning.** Corruption of training data to compromise AI model behaviour.
- (c) **Model theft.** Unauthorised access to or copying of AI models, including through API abuse.
- (d) **Deepfakes and synthetic media.** Use of AI to generate false or misleading audio, video, or images for deceptive purposes.
- (e) **AI-powered phishing.** Use of AI to generate highly convincing phishing emails or messages.
- (f) **Automated exploitation.** Use of AI to discover and exploit system vulnerabilities at scale.
- (g) **Model inversion.** Extraction of sensitive information about training data through AI model queries.
- (h) **Supply chain risks.** Risks arising from third-party AI components, libraries, or services.

The ICT Directorate shall maintain a risk register of AI-related cybersecurity threats and shall update it regularly.

23.3 Protection of AI Systems from Unauthorised Access

The University shall implement appropriate access controls for AI systems, including:

- (a) **Authentication.** Strong authentication mechanisms for accessing AI systems, including multi-factor authentication where appropriate.
- (b) **Authorisation.** Role-based access controls that limit access to AI systems and data based on the principle of least privilege.

- (c) **Audit logging.** Comprehensive logging of access to and use of AI systems, as required by Section 20.7.
- (d) **Network security.** Network segmentation and firewalls to protect AI systems from unauthorised external access.
- (e) **Physical security.** Physical security measures for AI infrastructure, including servers and workstations.
- (f) **Regular reviews.** Regular reviews of access controls to ensure that permissions remain appropriate and that access by departed staff or students is revoked promptly.

23.4 Secure Development and Deployment Practices

The University shall adopt secure development and deployment practices for AI systems. These shall include:

- (a) **Security by design.** Consideration of security requirements from the earliest stages of AI system design and development.
- (b) **Threat modelling.** Systematic identification and assessment of potential threats to AI systems.
- (c) **Security testing.** Regular security testing, including penetration testing, before deployment and periodically thereafter.
- (d) **Vulnerability management.** Prompt identification and remediation of vulnerabilities in AI systems and their dependencies.
- (e) **Change management.** Controlled processes for updating AI models, data, and configurations, with appropriate testing and approval.
- (f) **Incident response.** Procedures for responding to AI-related security incidents, as detailed in Section 23.4.

23.5 Incident Response for AI-Related Security Breaches

The University shall establish incident response procedures for AI-related security breaches. These procedures shall:

- (a) **Define AI-related incidents.** Include unauthorised access to AI systems, data breaches involving AI-processed data, AI system failures, and malicious AI use.
- (b) **Establish reporting mechanisms.** Provide clear channels for reporting suspected AI-related security incidents.
- (c) **Ensure prompt investigation.** Require prompt investigation of reported incidents to determine their scope, cause, and impact.
- (d) **Contain and remediate.** Include measures to contain incidents and remediate their effects, including the ability to disable or suspend AI systems where necessary.
- (e) **Notify as required.** Comply with breach notification requirements under the NDPA and the Cybercrimes (Amendment) Act 2024.
- (f) **Document and learn.** Require documentation of all incidents and lessons learned, with periodic review to improve incident response capabilities.

The ICT Directorate shall lead incident response for AI-related security breaches, in coordination with the DPO and the AI Policy Committee.

23.6 Compliance with the Cybercrimes (Amendment) Act 2024

The University shall comply with the Cybercrimes (Amendment) Act 2024. In relation to AI, this includes:

- (a) **Prohibition of unauthorised access.** Ensuring that AI systems are not used to gain unauthorised access to computer systems or data.
- (b) **Prohibition of data interference.** Ensuring that AI systems are not used to interfere with data or computer systems without authorisation.
- (c) **Prohibition of fraud.** Ensuring that AI systems are not used for fraudulent purposes, including identity theft and financial fraud.
- (d) **Cooperation with authorities.** Cooperating with law enforcement authorities in the investigation of AI-related cybercrimes.
- (e) **Awareness and training.** Providing cybersecurity awareness training that addresses AI-related risks, including the risks of using AI tools that may facilitate criminal activity.

23.7 Prohibition on Malicious AI Use

The University prohibits the use of AI for malicious purposes. Prohibited uses include:

- (a) **Generating malware.** Using AI to create, modify, or distribute malicious software.
- (b) **Conducting attacks.** Using AI to conduct cyberattacks, including denial-of-service attacks and automated exploitation.
- (c) **Creating deepfakes.** Using AI to create deepfakes or synthetic media for deceptive, defamatory, or harmful purposes.
- (d) **Automating harassment.** Using AI to generate or disseminate harassing, threatening, or abusive content.
- (e) **Circumventing security controls.** Using AI to bypass or defeat security controls, including authentication and access controls.
- (f) **Engaging in academic dishonesty at scale.** Using AI to systematically commit or facilitate academic misconduct.

Violations of this prohibition shall be treated as serious misconduct and shall be subject to disciplinary action, as well as referral to law enforcement authorities where appropriate.

23.8 Staff and Student Cybersecurity Awareness

The University shall provide cybersecurity awareness training to all staff and students, with specific content addressing AI-related risks. This training shall cover:

- (a) **Recognising AI-powered threats.** How to identify phishing, deepfakes, and other AI-powered attacks.
- (b) **Secure AI use.** How to use AI tools securely, including protecting credentials and avoiding disclosure of sensitive information.

- (c) **Reporting incidents.** How to report suspected AI-related security incidents.
- (d) **Legal obligations.** Understanding the legal obligations under the Cybercrimes (Amendment) Act 2024 and the NDPA.
- (e) **Consequences of misuse.** Understanding the consequences of malicious AI use for individuals and the University.

Training shall be provided as part of induction and through periodic refresher sessions. The ICT Directorate, in collaboration with the Human Resources Unit and the AI Policy Committee, shall coordinate the delivery of this training.

Section 24: Risk Management Framework

24.1 Foundational Position

McPherson University adopts a risk-based approach to AI governance. The University recognises that not all AI applications carry the same level of risk, and that governance measures should be proportionate to the risks involved. This Section establishes the framework for identifying, assessing, mitigating, and monitoring AI-related risks at the University.

The University's risk management approach is aligned with the NUC's emphasis on strengthening institutional data governance and enforcing compliance through periodic monitoring, as well as with international best practice, including the OECD AI Principles and the US AI Risk Management Framework.

24.2 AI Risk Identification and Assessment

The University shall establish processes for identifying and assessing AI-related risks. These processes shall include:

- (a) **Risk identification.** Systematic identification of potential risks associated with AI systems, including ethical, legal, operational, reputational, security, and privacy risks.
- (b) **Risk assessment.** Assessment of the likelihood and potential impact of identified risks, using a consistent risk assessment methodology.
- (c) **Risk categorisation.** Categorisation of AI systems based on their risk level (low, medium, high, or critical), with differentiated governance requirements for each category.
- (d) **Risk documentation.** Documentation of risk assessments, including the basis for risk ratings and the measures proposed to mitigate identified risks.
- (e) **Risk review.** Regular review of risk assessments to ensure that they remain accurate and up to date, particularly when AI systems are modified or when the operating environment changes.

The AI Policy Committee shall establish and maintain a risk assessment methodology and shall provide guidance to units on conducting risk assessments for AI systems.

24.3 Risk Categorisation

The University shall categorise AI risks according to the following framework:

Low Risk. AI applications that have minimal potential for harm and do not process personal data or affect individual rights. Examples include AI-assisted grammar checking, scheduling tools, and general productivity applications.

Medium Risk. AI applications that process personal data, affect individual rights or privileges, or have the potential to cause moderate harm if they fail. Examples include AI-assisted marking, academic advising tools, and administrative decision-support systems.

High Risk. AI applications that make or significantly influence decisions affecting individual rights, access, or opportunities; that process sensitive personal data; or that have the potential to cause significant harm. Examples include AI in admissions, performance management, or automated decision-making systems.

Critical Risk. AI applications that support critical University functions, that could cause severe harm if compromised or manipulated, or that are subject to stringent regulatory requirements. Examples include AI systems supporting examination administration, financial management, or security operations.

Differentiated governance requirements for each risk category shall be specified in the AI Policy Committee's guidance.

24.4 Risk Mitigation Strategies

The University shall implement risk mitigation strategies proportionate to the level of risk. These may include:

- (a) **Technical controls.** Access controls, encryption, audit logging, and other technical measures to reduce risk.
- (b) **Organisational controls.** Policies, procedures, training, and oversight arrangements to manage risk.
- (c) **Human oversight.** Requirements for human review and approval of AI-assisted decisions, particularly for high-risk applications.
- (d) **Transparency and disclosure.** Measures to ensure that AI use is transparent and that affected individuals are informed.
- (e) **Contingency planning.** Plans for responding to AI system failures, security incidents, or ethical concerns.
- (f) **Insurance.** Consideration of insurance arrangements for high-risk AI applications, where appropriate.
- (g) **Discontinuation.** Where risks cannot be adequately mitigated, the University may decide not to deploy or to discontinue an AI system.

24.5 AI System Registration and Inventory

The University shall maintain a register of all AI systems deployed by the University. This register shall include:

- (a) The name and description of the AI system;
- (b) The unit or units responsible for the system;
- (c) The purpose and scope of the system;
- (d) The categories of data processed;

- (e) The risk categorisation of the system;
- (f) The human oversight arrangements;
- (g) The date of deployment and any review dates;
- (h) Any applicable data processing agreements or security assessments.

The ICT Directorate, in collaboration with the AI Policy Committee, shall maintain this register. Units deploying AI systems shall ensure that their systems are registered and that the register is kept up to date.

24.6 Regular Risk Reviews and Audits

The University shall conduct regular risk reviews and audits of AI systems. These shall include:

- (a) **Annual risk reviews.** Annual review of risk assessments for all AI systems, with more frequent reviews for high-risk and critical-risk systems.
- (b) **Internal audits.** Periodic internal audits of AI systems to verify compliance with this policy and applicable legal requirements.
- (c) **External audits.** Where appropriate, external audits of AI systems by qualified independent auditors.
- (d) **Post-incident reviews.** Reviews following AI-related incidents to identify lessons learned and improve risk management.
- (e) **Compliance monitoring.** Ongoing monitoring of compliance with this policy, including through the reporting mechanisms in Section 31.

The AI Policy Committee shall oversee the risk review and audit programme and shall report to the Senate as required.

24.7 Insurance and Liability Considerations

The University shall consider insurance and liability issues associated with AI systems. This shall include:

- (a) **Insurance coverage.** Reviewing existing insurance policies to determine whether they cover AI-related risks, and considering additional coverage where appropriate.
- (b) **Liability allocation.** Clarifying liability for AI-related harm, including through contractual arrangements with vendors and service providers.
- (c) **Indemnification.** Ensuring that vendor agreements include appropriate indemnification provisions for AI-related losses.
- (d) **Legal review.** Seeking legal advice on liability issues associated with AI systems, particularly for high-risk and critical-risk applications.

24.8 Business Continuity and Disaster Recovery for AI Systems

The University shall develop and maintain business continuity and disaster recovery plans for AI systems, particularly for systems supporting critical functions. These plans shall include:

- (a) **Continuity arrangements.** Arrangements for maintaining or restoring AI-supported functions during disruptions.

- (b) **Recovery procedures.** Procedures for recovering AI systems and data after failures or disasters.
- (c) **Testing.** Regular testing of business continuity and disaster recovery plans.
- (d) **Roles and responsibilities.** Clear definition of roles and responsibilities for business continuity and disaster recovery.
- (e) **Communication plans.** Plans for communicating with affected stakeholders during and after disruptions.

The ICT Directorate shall lead the development of these plans, in coordination with the AI Policy Committee and relevant units.

Section 25: Third-Party AI Tools and Services

25.1 Foundational Position

McPherson University recognises that much AI capability is delivered through third-party tools and services. The University's approach to third-party AI is therefore permissive but regulated: staff and students may use third-party AI tools where appropriate, subject to the requirements of this policy, but the University shall ensure that such use does not compromise its data, security, or values.

The University notes that the NDPA and GAID impose specific requirements for the deployment of emerging technologies, including AI, in personal data processing, and that the University must therefore exercise due diligence in the selection and management of third-party AI services.

25.2 Approved AI Tools and Platforms

The University shall maintain a list of approved AI tools and platforms. This list shall be developed and maintained by the ICT Directorate in consultation with the AI Policy Committee and shall be published to the University community.

Approval shall be based on:

- (a) **Security assessment.** Assessment of the tool's security features, including data encryption, access controls, and vulnerability management.
- (b) **Privacy assessment.** Assessment of the tool's data protection practices, including compliance with the NDPA and the GAID.
- (c) **Ethical assessment.** Assessment of the tool's alignment with the University's values and ethical principles.
- (d) **Functional assessment.** Assessment of the tool's suitability for its intended purposes.
- (e) **Cost assessment.** Assessment of the tool's cost-effectiveness and sustainability.

Tools that are not on the approved list may be used only with explicit authorisation from the AI Policy Committee, subject to appropriate safeguards.

25.3 Evaluation Criteria for Third-Party AI Services

The University shall apply the following evaluation criteria when assessing third-party AI services:

- (a) **Data protection.** The service provider's data protection practices, including compliance with the NDPA, data processing agreements, and data subject rights.
- (b) **Data ownership.** Clarity regarding ownership of data processed by the service, including whether the provider uses University data for its own purposes.
- (c) **Data location.** The locations where data is stored and processed, and compliance with data localisation requirements.
- (d) **Security.** The provider's security practices, including encryption, access controls, and incident response.
- (e) **Transparency.** The provider's transparency regarding its AI models, training data, and limitations.
- (f) **Reliability.** The provider's track record, service levels, and financial stability.
- (g) **Ethical practices.** The provider's ethical practices, including its approach to bias, fairness, and human rights.
- (h) **Support and training.** The provider's support arrangements and training resources.
- (i) **Exit and portability.** The ease of exiting the service and porting data to alternative solutions.

25.4 Data Processing Agreements with Vendors

Contracts with third-party AI service providers shall include data processing agreements that comply with the NDPA and the GAID. These agreements shall address:

- (a) **Processing instructions.** The University's instructions regarding the processing of personal data.
- (b) **Confidentiality.** The provider's obligation to maintain the confidentiality of University data.
- (c) **Security measures.** The technical and organisational measures the provider shall implement to protect University data.
- (d) **Sub-processors.** Arrangements for sub-processors, including the requirement for University approval.
- (e) **Data subject rights.** The provider's assistance with data subject rights requests.
- (f) **Breach notification.** The provider's obligation to notify the University of data breaches without undue delay.
- (g) **Audit rights.** The University's right to audit the provider's compliance with the agreement.
- (h) **Return or deletion of data.** Arrangements for the return or deletion of University data upon termination.

The University's Legal Unit and ICT Directorate shall review data processing agreements to ensure compliance with these requirements.

25.5 Vendor Security and Privacy Assessments

Before procuring a third-party AI service, the University shall conduct a security and privacy assessment of the vendor. This assessment shall include:

- (a) **Security questionnaire.** A standardised questionnaire covering the vendor's security practices, certifications, and incident history.

(b) **Privacy review.** A review of the vendor's privacy policies, data processing practices, and compliance with the NDPA.

(c) **Reference checks.** Where appropriate, reference checks with other institutional users of the vendor's services.

(d) **Demonstration or trial.** Where feasible, a demonstration or trial of the service to assess its security and privacy features in practice.

(e) **Documentation review.** Review of the vendor's security and privacy documentation, including certifications and audit reports.

The results of these assessments shall be documented and shall inform the procurement decision.

25.6 Prohibition on Unauthorised AI Tool Use

The University prohibits the use of unauthorised AI tools for University-related activities, particularly where such use involves:

(a) **Confidential or sensitive data.** Uploading confidential, sensitive, or restricted University data to unauthorised AI tools.

(b) **Personal data.** Processing personal data using AI tools that have not been assessed for compliance with the NDPA.

(c) **University business.** Using unauthorised AI tools to conduct University business, including administrative, academic, or research activities.

(d) **Circumvention.** Using unauthorised AI tools to circumvent this policy or other University policies.

Staff and students shall use only approved AI tools for University-related activities, except where explicit authorisation has been obtained from the AI Policy Committee.

25.7 Monitoring and Review of Third-Party AI Services

The University shall monitor and review third-party AI services on an ongoing basis. This shall include:

(a) **Performance monitoring.** Monitoring the performance of AI services against service level agreements.

(b) **Security monitoring.** Monitoring for security incidents, vulnerabilities, and changes in the vendor's security posture.

(c) **Privacy monitoring.** Monitoring for changes in the vendor's privacy practices or compliance status.

(d) **Terms monitoring.** Monitoring for changes in the vendor's terms of service that may affect the University's rights or obligations.

(e) **Periodic review.** Periodic review of each AI service to determine whether it continues to meet the University's needs and standards.

The ICT Directorate shall be responsible for monitoring third-party AI services and shall report to the AI Policy Committee on any issues identified.

25.8 Exit Strategies and Data Portability

The University shall maintain exit strategies for third-party AI services, particularly for services that process critical or sensitive data. These strategies shall include:

- (a) **Data portability.** Ensuring that University data can be exported from the service in a usable format.
- (b) **Transition planning.** Planning for the transition to alternative services or in-house solutions.
- (c) **Data deletion.** Ensuring that University data is securely deleted from the vendor's systems upon termination.
- (d) **Continuity.** Arrangements to maintain continuity of operations during and after transition.
- (e) **Contractual provisions.** Ensuring that contracts include provisions for exit and data portability.

The University shall not become dependent on any single third-party AI service for critical functions without a viable exit strategy.

Part Eight: Capacity Building and Culture

Section 26: AI Literacy and Training

26.1 Foundational Position

McPherson University affirms that the successful and responsible adoption of Artificial Intelligence depends not merely on infrastructure, policies, or tools, but on the capabilities, confidence, and ethical awareness of the people who use them. The University's vision of building "a people of excellence and integrity for service" requires that AI capacity building be pursued with the same seriousness as AI infrastructure development.

This Section establishes the University's framework for AI literacy and training. The framework is grounded in the recognition that AI competencies must be developed across the entire University community — students, academic staff, administrative staff, technical staff, and management — and must address not only technical skills but also ethical reasoning, critical evaluation, and disciplinary application.

The University notes the NUC's emphasis on enhanced human capacity development for AI across the Nigerian University System, as articulated at the NAAIP symposium and reflected in the Commission's own internal capacity-building initiatives, including its January 2026 training for management staff on AI applications in policy formulation, decision-making, and operational efficiency. The University aligns with this national direction and commits to building the AI competencies of its own community.

The University further notes the Nigeria National Artificial Intelligence Strategy's target of equipping at least 70% of Nigeria's young workforce aged 16–35, including 50% women, with AI-related skills by 2030. McPherson University shall contribute to this national objective by ensuring that its graduates and staff possess the AI competencies required for the emerging economy.

26.2 Baseline AI Literacy for All Students

McPherson University shall ensure that every student, regardless of discipline or programme, acquires foundational AI literacy during their studies. This commitment is consistent with the NUC's direction that AI competencies and ethics be integrated across disciplines under the Core Curriculum and Minimum Academic Standards (CCMAS), and with the emerging consensus in West African higher education that AI literacy must integrate technical skills with ethical principles and culturally appropriate strategies.

The baseline AI literacy requirement shall include:

- (a) **Conceptual understanding.** Students shall understand what AI is, how it works at a foundational level, the different categories of AI systems, and the distinction between narrow AI and general AI.
- (b) **Practical competence.** Students shall be able to use AI tools effectively for learning, research, and problem-solving within their disciplines.
- (c) **Critical evaluation.** Students shall be able to evaluate AI outputs for accuracy, reliability, bias, and appropriateness, and to recognise the limitations of AI systems.
- (d) **Ethical reasoning.** Students shall understand the ethical implications of AI use, including issues of academic integrity, privacy, bias, and the social impacts of AI.

(e) **Disciplinary application.** Students shall understand how AI is applied within their field of study and the professional and regulatory standards governing AI use in that field.

The baseline AI literacy requirement may be satisfied through a combination of dedicated modules, embedded content within existing courses, co-curricular activities, and self-directed learning, as determined by the Senate on the recommendation of the AI Policy Committee and the Committee of Deans.

26.3 AI Competency Framework for Staff

McPherson University shall adopt a competency framework for staff AI literacy that distinguishes between different roles and levels of responsibility. This framework is informed by international best practice, including UNESCO's AI competency frameworks for students and teachers, which emphasise a human-centred mindset, ethics of AI, AI techniques and applications, and AI system design.

The University's staff AI competency framework shall include four levels:

Level One — AI Aware. All staff shall possess basic awareness of AI, its capabilities, its limitations, and its ethical implications. This level is required for all staff as a condition of employment.

Level Two — AI Competent. Staff in roles that involve regular interaction with AI tools shall possess practical competence in using AI for their work, including the ability to evaluate AI outputs and use AI responsibly.

Level Three — AI Proficient. Staff who design, deploy, or manage AI systems, or who teach AI-related content, shall possess advanced competence in AI, including deep understanding of AI capabilities, limitations, risks, and governance requirements.

Level Four — AI Leader. Staff who lead AI initiatives, serve on AI governance bodies, or provide AI-related training to others shall possess expert-level competence and shall contribute to the University's AI knowledge base and external engagement.

The AI Policy Committee shall publish detailed competency descriptors for each level and shall establish mechanisms for staff to assess their current level and plan their development.

26.4 Role-Specific Training

The University shall provide role-specific AI training tailored to the needs of different staff categories:

(a) **Academic staff.** Training shall cover AI in teaching and learning, AI-resilient assessment design, AI in research and publication, ethical issues in AI use, and discipline-specific AI applications. The University notes research indicating that while general-purpose AI tools such as ChatGPT are widely used by Nigerian academics, advanced research tools remain underutilised, and that inadequate infrastructure, lack of institutional policies, and limited digital literacy are significant barriers to effective AI adoption. Training shall therefore address both foundational and advanced AI applications, and shall be designed to close the adoption gap.

(b) **Administrative staff.** Training shall cover AI for administrative efficiency, responsible use of AI in administrative decisions, data protection in AI use, and the limits of AI in administrative contexts.

(c) **ICT staff.** Training shall cover AI infrastructure management, AI security, AI system integration, and technical aspects of AI governance.

(d) **Library staff.** Training shall cover AI in information literacy, AI research tools, AI citation and attribution, and support for students and staff in AI-related learning.

(e) **Management staff.** Training shall cover strategic AI leadership, AI governance, AI investment decisions, and the NUC's AI policy framework. The University notes the NUC's own management training initiative, which focused on AI applications in policy formulation, decision-making, operational efficiency, and workplace productivity, and shall provide equivalent or superior training for its own management team.

(f) **Research staff and postgraduate students.** Training shall cover AI in research methodology, AI ethics in research, responsible AI use in publication, and discipline-specific AI research tools.

26.5 Continuing Professional Development in AI

The University recognises that AI is a rapidly evolving field and that one-time training is insufficient. The University shall establish a continuing professional development (CPD) programme for AI that includes:

(a) **Annual refresher training.** All staff shall participate in annual AI refresher training to stay current with developments, policy changes, and emerging risks.

(b) **Periodic advanced training.** Staff shall have access to advanced AI training opportunities on a periodic basis, tailored to their roles and development needs.

(c) **Seminar and workshop series.** The University shall host regular seminars and workshops on AI developments, featuring internal and external experts.

(d) **Online learning resources.** The University shall curate and provide access to online AI learning resources, including courses, tutorials, and documentation.

(e) **External training opportunities.** The University shall support staff participation in external AI training programmes, conferences, and professional development activities, subject to available resources.

The Human Resources Unit, in collaboration with the ICT Directorate and the AI Policy Committee, shall coordinate the CPD programme and shall maintain records of staff participation.

26.6 Certification and Recognition of AI Competencies

The University shall establish mechanisms for recognising and certifying AI competencies acquired by staff and students. This may include:

(a) **Internal certification.** The University may issue certificates or digital badges for completion of AI training programmes and demonstration of competencies.

(b) **External certification support.** The University shall encourage and support staff and students in obtaining relevant external AI certifications.

(c) **Recognition in performance review.** AI competency development shall be recognised in staff performance reviews and promotion considerations.

(d) **Student recognition.** AI competency achievements shall be recognised in student records and co-curricular transcripts where appropriate.

26.7 Training Resources and Delivery Mechanisms

The University shall develop and maintain training resources and delivery mechanisms for AI capacity building. These shall include:

- (a) **Online learning platform.** The University shall use its learning management system or a dedicated platform to deliver AI training content asynchronously.
- (b) **In-person workshops.** The University shall conduct in-person workshops for hands-on AI training and for topics requiring interactive discussion.
- (c) **Peer learning networks.** The University shall establish communities of practice for staff and students to share AI knowledge and experiences.
- (d) **Training materials.** The University shall develop and curate training materials, including guides, case studies, and practical exercises, tailored to the University's context and disciplines.
- (e) **Train-the-trainer programmes.** The University shall develop internal capacity to deliver AI training through train-the-trainer programmes.

The University notes that its existing partnership discussions with BEE Solutions and Consultancy Services include provisions for training administrative and technical staff in artificial intelligence, modern administrative practices, and paperless office systems. The University shall leverage such partnerships to supplement its internal training capacity.

Section 27: Awareness and Communication

27.1 Foundational Position

McPherson University recognises that policy effectiveness depends on awareness. A policy that is not known, understood, and internalised by the University community cannot achieve its objectives. The University shall therefore implement a comprehensive awareness and communication strategy for AI, ensuring that all members of the community understand this policy, their responsibilities under it, and the resources available to support responsible AI use.

27.2 Communicating the Policy to the University Community

The University shall communicate this policy to all members of the University community through:

- (a) **Official launch and dissemination.** The policy shall be officially launched and disseminated through University channels, including the University website, email, and physical noticeboards.
- (b) **Orientation sessions.** Orientation sessions shall be conducted for staff and students to introduce the policy, explain its requirements, and address questions.
- (c) **Integration into handbooks.** The policy shall be integrated into the Staff Handbook, Student Handbook, and other relevant University publications.
- (d) **Departmental briefings.** Deans and Heads of Department shall conduct departmental briefings to ensure that all staff understand the policy and its implications for their work.
- (e) **Student engagement.** Student representative bodies shall be engaged to disseminate the policy and to provide feedback on its implementation.

27.3 Regular Updates on AI Developments

The University shall provide regular updates to the University community on AI developments relevant to the institution. These updates shall include:

- (a) **New AI tools and resources.** Information about new AI tools and resources that are approved for use or that may be of interest to the community.
- (b) **Policy developments.** Updates on changes to this policy, NUC guidance, national regulations, and international standards.
- (c) **Emerging risks and threats.** Alerts about AI-related security risks, ethical concerns, or emerging issues.
- (d) **Success stories and best practices.** Sharing of examples of effective and responsible AI use within the University community.
- (e) **Training opportunities.** Announcements of upcoming AI training, workshops, and seminars.

The AI Policy Committee, in collaboration with the ICT Directorate and the University's communications unit, shall be responsible for preparing and disseminating these updates.

27.4 Sharing of Best Practices

The University shall encourage the sharing of best practices in AI use across Colleges, departments, and units. Mechanisms for sharing shall include:

- (a) **Communities of practice.** Established forums for staff and students to share AI experiences, tools, and approaches.
- (b) **Showcase events.** Periodic events where staff and students present AI-related projects and innovations.
- (c) **Internal publications.** Articles and reports in University publications highlighting effective AI practices.
- (d) **Cross-departmental collaboration.** Encouragement of collaboration between Colleges and units on AI-related initiatives.
- (e) **External dissemination.** Encouragement of staff to share McPherson University's AI experiences through conferences, publications, and professional networks.

27.5 Student and Staff Engagement Mechanisms

The University shall establish mechanisms for ongoing engagement with students and staff on AI-related matters. These shall include:

- (a) **Feedback channels.** Accessible channels for students and staff to provide feedback on AI policy, practices, and tools.
- (b) **Consultation processes.** Consultation with student and staff representatives on significant AI decisions, including the adoption of new AI tools and changes to policy.
- (c) **AI forums.** Periodic forums where students and staff can raise concerns, ask questions, and contribute to AI governance discussions.

(d) **Survey mechanisms.** Periodic surveys to assess AI awareness, attitudes, and needs within the University community.

(e) **Student representation.** Inclusion of student representatives in AI-related committees and working groups where appropriate.

27.6 External Communication and Public Engagement

The University shall communicate its AI activities and positions to external audiences through:

(a) **Website publication.** Publication of this policy and related AI resources on the University website, contributing to the University's NUC ranking profile and demonstrating institutional commitment to AI governance.

(b) **Press and media engagement.** Engagement with media to share the University's AI initiatives and perspectives.

(c) **Professional and academic networks.** Participation in national and international networks focused on AI in higher education.

(d) **Community engagement.** Engagement with the local community, industry, and other stakeholders on AI-related matters.

(e) **Regulatory engagement.** Communication with NUC, NITDA, and other regulatory bodies on AI governance matters.

27.7 Integration with University Website and NUC Ranking Requirements

The University recognises that the public availability of its AI policy and related documentation contributes to institutional transparency and may be considered in NUC ranking assessments. The University shall therefore ensure that:

(a) **Policy publication.** This policy is published on the University website in an accessible format.

(b) **Supporting resources.** Supporting resources, including training materials, guidelines, and FAQs, are published alongside the policy.

(c) **Regular updates.** The published policy and resources are updated as required.

(d) **Accessibility.** Published materials are accessible to persons with disabilities and are available in accessible formats.

(e) **Archival.** Historical versions of the policy are archived and accessible for reference.

Section 28: Research and Innovation Promotion

28.1 Foundational Position

McPherson University affirms that research and innovation are essential to its mission of providing qualitative, functional, and sound education. The University's vision of building "a people of excellence and integrity for service" extends to its research enterprise, and the University is committed to promoting research that addresses developmental challenges in Nigeria and across Africa.

The University recognises that Artificial Intelligence presents significant opportunities for research and innovation across all disciplines. This Section establishes the University's commitment to promoting AI-related research and innovation, and to creating an enabling environment for faculty and students to engage in cutting-edge AI scholarship.

The University notes its ongoing discussions with BEE Solutions and Consultancy Services regarding a strategic partnership to strengthen capacity development, promote research excellence, and create opportunities for international collaboration, with a focus on training in grant writing and promoting high-impact research to address developmental challenges in Nigeria and across Africa. The University shall build on such partnerships to advance its AI research agenda.

28.2 Encouraging AI-Related Research

The University shall encourage AI-related research across all Colleges and disciplines. This encouragement shall take the form of:

- (a) **Research funding priorities.** The University shall include AI-related research among its research funding priorities, subject to available resources.
- (b) **Seed funding.** The University shall establish seed funding opportunities for AI-related research projects, particularly for early-career researchers.
- (c) **Recognition and reward.** The University shall recognise and reward staff who produce high-quality AI-related research, including through research awards and promotion criteria.
- (d) **Research leave and sabbaticals.** The University shall support staff seeking research leave or sabbaticals to pursue AI-related research.
- (e) **Conference support.** The University shall provide support for staff to present AI-related research at national and international conferences.

28.3 Interdisciplinary AI Research Initiatives

The University shall promote interdisciplinary AI research that brings together expertise from different Colleges and disciplines. This shall include:

- (a) **Interdisciplinary research clusters.** Establishment of research clusters focused on AI applications in areas such as health, agriculture, education, governance, and business.
- (b) **Cross-College collaboration.** Encouragement of collaboration between the College of Computing and other Colleges on AI-related research.
- (c) **Joint research proposals.** Support for the development of joint research proposals that integrate AI with disciplinary expertise from multiple fields.
- (d) **Shared research resources.** Provision of shared research resources, including computing facilities and datasets, to support interdisciplinary AI research.
- (e) **Interdisciplinary seminars and workshops.** Organisation of seminars and workshops that bring together researchers from different disciplines to explore AI-related themes.

28.4 Collaboration with Industry and Other Institutions

The University shall promote collaboration with industry, government, and other academic institutions on AI-related research and innovation. This shall include:

- (a) **Industry partnerships.** Development of partnerships with industry partners on AI research, development, and application.
- (b) **Government collaboration.** Collaboration with government agencies on AI-related research and policy development.
- (c) **Inter-university collaboration.** Collaboration with other Nigerian and African universities on AI research and capacity building.
- (d) **International collaboration.** Collaboration with international partners on AI research, subject to the data protection and ethical requirements of this policy.
- (e) **Joint funding applications.** Support for joint funding applications with external partners for AI-related research.

The University's Research Office shall facilitate these collaborations and shall maintain a register of active AI-related partnerships.

28.5 AI Innovation and Entrepreneurship

The University shall promote AI innovation and entrepreneurship among staff and students. This shall include:

- (a) **Innovation challenges.** Organisation of AI innovation challenges and hackathons that encourage creative problem-solving.
- (b) **Incubation support.** Provision of incubation support for AI-related startups and social enterprises developed by staff or students.
- (c) **Entrepreneurship training.** Integration of AI-related entrepreneurship content into relevant programmes and co-curricular activities.
- (d) **Mentorship.** Connection of aspiring AI entrepreneurs with mentors from industry and the University's alumni network.
- (e) **Intellectual property support.** Support for the protection and commercialisation of AI-related intellectual property developed at the University, in accordance with the University's Intellectual Property Policy.

28.6 Funding and Resource Support for AI Research

The University shall mobilise resources to support AI-related research. This shall include:

- (a) **Internal research grants.** Allocation of internal research grants for AI-related projects.
- (b) **External funding support.** Support for staff in identifying and applying for external funding for AI research, including from TETFund, research councils, international foundations, and industry partners.
- (c) **Equipment and infrastructure.** Provision of equipment and infrastructure to support AI research, as detailed in Section 22.

(d) **Research assistance.** Provision of research assistants and technical support for AI-related projects where feasible.

(e) **Library resources.** Provision of library resources, including AI journals, databases, and tools, to support AI research.

28.7 Dissemination and Knowledge Sharing

The University shall promote the dissemination and sharing of AI-related knowledge generated through its research. This shall include:

(a) **Publication support.** Support for staff and students to publish AI-related research in reputable journals and conference proceedings.

(b) **Open access.** Encouragement of open access publication for AI-related research, subject to funder and publisher requirements.

(c) **Seminars and conferences.** Organisation of seminars, conferences, and workshops to share AI research findings.

(d) **Policy engagement.** Engagement with policymakers to translate AI research findings into policy recommendations.

(e) **Community engagement.** Sharing of AI research findings with the broader community through accessible formats and public engagement activities.

(f) **Repository.** Maintenance of an institutional repository for AI-related research outputs, accessible to the University community and, where appropriate, to the public.

Part Nine: Governance and Accountability

Section 29: Governance Structure

29.1 Foundational Position

McPherson University affirms that the effective governance of Artificial Intelligence requires clear structures, defined roles, and accountable decision-making. The University notes that the NUC's Artificial Intelligence Policy Framework and Implementation Roadmap emphasises the establishment of AI governance committees and annual Senate policy review cycles as key mechanisms for institutional AI oversight. The NUC has also stated that it will enforce compliance through periodic monitoring of university AI development and mandatory capacity-building programmes.

The University further notes the directive from the Committee of Pro-Chancellors of State-Owned Universities (COPSUN) urging university leadership to establish AI and Digital Governance Committees to drive AI adoption and ensure responsible governance. Although McPherson University is a private institution, the University recognises the value of this guidance and adopts a governance structure consistent with national expectations.

This Section establishes the governance architecture for AI at McPherson University. The structure is designed to ensure that AI-related decisions are made transparently, that responsibility is clearly allocated, and that the University community has accessible channels for raising concerns and seeking guidance.

29.2 University Senate

The Senate of McPherson University is the supreme academic governance body of the University. In relation to AI, the Senate shall:

- (a) **Approve and amend this policy.** The Senate holds ultimate authority over the content and provisions of this policy.
- (b) **Provide strategic oversight.** The Senate shall provide strategic direction for AI adoption and governance at the University.
- (c) **Receive and consider reports.** The Senate shall receive annual reports from the AI Policy Committee on the implementation of this policy, AI-related developments, and compliance matters.
- (d) **Conduct periodic policy review.** The Senate shall conduct a comprehensive review of this policy at least every two years, or more frequently if circumstances require.
- (e) **Approve major AI investments.** The Senate shall approve significant AI-related investments, partnerships, and initiatives as recommended by the AI Policy Committee and the University Management.
- (f) **Ensure alignment with mission.** The Senate shall ensure that AI adoption at the University remains consistent with the University's mission, vision, and values.

The Senate's role in AI governance is consistent with the NUC's emphasis on retaining human judgment in academic decisions and ensuring that AI serves, rather than supplants, academic governance.

29.3 AI Policy Committee

The University shall establish an AI Policy Committee as the principal operational body for AI governance. The Committee shall be constituted by the Senate and shall report to the Senate through the Vice-Chancellor.

Composition. The AI Policy Committee shall comprise:

- (a) A Chairperson, appointed by the Vice-Chancellor from among senior academic staff with relevant expertise;
- (b) The Deputy Vice-Chancellor (Academic), or their representative;
- (c) The Director of ICT, or their representative;
- (d) The University Librarian, or their representative;
- (e) The Data Protection Officer;
- (f) One Dean representing each College, nominated by the Committee of Deans;
- (g) One representative of the Research Ethics Committee;
- (h) One representative of the Academic Planning Unit;
- (i) One representative of the Legal Unit;
- (j) One student representative, nominated by the Student Representative Council;
- (k) One representative of the non-academic staff, nominated by the relevant staff association;
- (l) Up to three co-opted members with relevant expertise, as determined by the Committee.

The Committee may invite external experts to advise on specific matters as required.

Mandate. The AI Policy Committee shall:

- (a) **Oversee policy implementation.** Monitor and coordinate the implementation of this policy across all Colleges and units.
- (b) **Develop guidance and procedures.** Prepare and publish operational guidance, templates, and procedures to support the implementation of this policy, including the five-category AI use scale, disclosure forms, and risk assessment methodologies.
- (c) **Review AI tools and services.** Evaluate and recommend AI tools and services for approval, in consultation with the ICT Directorate and the DPO.
- (d) **Conduct risk assessments.** Coordinate risk assessments for AI systems, in accordance with the risk categorisation framework in Section 24.
- (e) **Review DPIAs.** Review Data Privacy Impact Assessments conducted for AI systems, in collaboration with the DPO.
- (f) **Monitor compliance.** Monitor compliance with this policy and report to the Senate on compliance matters.
- (g) **Prepare NUC reports.** Prepare and submit the University's AI compliance reports to the NUC using the Commission's standardised reporting template.

(h) **Coordinate training and awareness.** Oversee the delivery of AI training and awareness programmes across the University.

(i) **Consider emerging issues.** Monitor AI developments and consider emerging ethical, legal, and operational issues, making recommendations to the Senate as appropriate.

(j) **Handle referrals.** Consider referrals from staff, students, and units on AI-related matters and provide guidance or recommendations.

(k) **Maintain the AI system register.** Maintain the University's register of AI systems, as required by Section 24.5.

(l) **Report annually.** Submit an annual report to the Senate on the state of AI governance at the University, including achievements, challenges, and recommendations for improvement.

Meetings. The AI Policy Committee shall meet at least once per semester, and more frequently as required. Minutes of meetings shall be maintained and shall be available to the Senate.

29.4 College AI Representatives

Each College shall designate a College AI Representative, who shall serve as the primary liaison between the College and the AI Policy Committee. The College AI Representative shall:

(a) **Disseminate information.** Communicate AI-related policies, guidance, and updates to staff and students within the College.

(b) **Coordinate training.** Coordinate AI training and awareness activities within the College.

(c) **Provide support.** Provide guidance and support to staff and students on AI-related matters.

(d) **Report concerns.** Report AI-related concerns, incidents, and emerging issues to the AI Policy Committee.

(e) **Facilitate compliance.** Facilitate compliance with this policy within the College, including the preparation of course-level AI use statements and the maintenance of AI system records.

(f) **Share best practices.** Share best practices and lessons learned within the College and with other Colleges through the AI Policy Committee.

College AI Representatives shall be appointed by the Dean of each College in consultation with the AI Policy Committee and shall serve for a renewable term of two years.

29.5 ICT Directorate

The ICT Directorate shall be responsible for the technical implementation of AI infrastructure, systems, and security at the University. In relation to AI, the ICT Directorate shall:

(a) **Manage AI infrastructure.** Manage the University's AI-related computing resources, networks, and cloud services.

(b) **Implement security measures.** Implement and maintain security measures for AI systems, in accordance with Section 23.

(c) **Maintain the AI system register.** Maintain the University's register of AI systems, in collaboration with the AI Policy Committee.

- (d) **Conduct security assessments.** Conduct security assessments of AI tools and services prior to procurement and periodically thereafter.
- (e) **Lead incident response.** Lead the response to AI-related security incidents, in coordination with the DPO and the AI Policy Committee.
- (f) **Provide technical support.** Provide technical support to staff and students using AI tools and systems.
- (g) **Monitor performance.** Monitor the performance and reliability of AI systems and report to the AI Policy Committee on any issues.
- (h) **Advise on procurement.** Provide technical advice on the procurement of AI tools and services.
- (i) **Support training.** Support the delivery of AI-related technical training for staff and students.

29.6 Data Protection Officer

The Data Protection Officer (DPO) shall be responsible for ensuring compliance with the Nigeria Data Protection Act 2023 and this policy in relation to the processing of personal data by AI systems. In relation to AI, the DPO shall:

- (a) **Advise on compliance.** Provide expert advice on data protection requirements for AI systems.
- (b) **Conduct and review DPIAs.** Conduct and review Data Privacy Impact Assessments for AI systems, in collaboration with the AI Policy Committee.
- (c) **Handle data subject rights.** Facilitate the exercise of data subject rights in relation to AI processing.
- (d) **Monitor compliance.** Monitor compliance with the NDPA and this policy in relation to AI processing.
- (e) **Lead breach response.** Lead the response to data breaches involving AI systems, in coordination with the ICT Directorate.
- (f) **Maintain records.** Maintain records of processing activities, DPIAs, and data breaches.
- (g) **Prepare compliance reports.** Prepare and submit the University's data protection compliance reports, including reports to the Nigeria Data Protection Commission.
- (h) **Deliver training.** Deliver data protection training with specific content on AI-related data protection issues.
- (i) **Report to the AI Policy Committee.** Report regularly to the AI Policy Committee on data protection matters relating to AI.

29.7 Research Ethics Committee

The Research Ethics Committee (REC) shall be responsible for the ethical review of research involving AI, as detailed in Section 13. In relation to AI, the REC shall:

- (a) **Review AI-related research.** Review research proposals involving AI to ensure compliance with ethical standards and this policy.
- (b) **Provide guidance.** Provide guidance to researchers on the ethical use of AI in research.
- (c) **Monitor approved research.** Monitor approved AI-related research to ensure continued compliance with ethical requirements.

(d) **Report concerns.** Report to the AI Policy Committee any ethical concerns arising from AI-related research.

(e) **Include AI expertise.** Ensure that the REC includes or has access to expertise in AI ethics and data protection.

29.8 Library and Information Services

The University Library shall support AI literacy and research by:

(a) **Curating AI resources.** Curating and providing access to AI-related books, journals, databases, and learning resources.

(b) **Providing research support.** Providing research support for AI-related projects, including literature searching and citation guidance.

(c) **Delivering information literacy.** Delivering information literacy training that includes AI-related content, including critical evaluation of AI outputs and citation of AI-assisted work.

(d) **Managing institutional repository.** Managing the University's institutional repository of AI-related research outputs.

(e) **Supporting students and staff.** Providing support to students and staff on AI-related information and research matters.

29.9 Student Affairs

The Student Affairs Unit shall support AI governance by:

(a) **Disseminating information.** Disseminating AI-related information to students through student channels.

(b) **Supporting student engagement.** Supporting student engagement with AI governance, including through the student representative on the AI Policy Committee.

(c) **Addressing student concerns.** Addressing student concerns related to AI use, including concerns about equity, privacy, and academic integrity.

(d) **Coordinating co-curricular activities.** Coordinating co-curricular AI-related activities, including student clubs and competitions.

(e) **Supporting student discipline.** Supporting the implementation of disciplinary procedures for AI-related academic misconduct, in accordance with Section 8.

29.10 Governing Council

The Governing Council of McPherson University, as the supreme governing body of the University, shall provide overarching oversight for AI governance. The Council shall:

(a) **Receive reports.** Receive reports from the Senate on AI governance matters, including the annual AI governance report.

(b) **Approve major investments.** Approve significant AI-related investments and partnerships, as recommended by the Senate and Management.

(c) **Ensure alignment with institutional mission.** Ensure that AI adoption remains consistent with the University's mission, vision, and values.

(d) **Provide strategic direction.** Provide strategic direction for AI adoption and governance at the highest level of the University.

29.11 External Advisory Engagement

The University may establish an External AI Advisory Panel comprising experts from industry, academia, government, and civil society to provide independent advice on AI governance matters. The Panel shall:

(a) **Provide expert advice.** Provide advice on emerging AI developments, regulatory trends, and best practices.

(b) **Review University AI practices.** Review the University's AI governance practices and make recommendations for improvement.

(c) **Facilitate partnerships.** Facilitate partnerships with external organisations on AI-related initiatives.

(d) **Enhance credibility.** Enhance the credibility and transparency of the University's AI governance through independent oversight.

The Panel shall be advisory in nature and shall not have decision-making authority. Its recommendations shall be considered by the AI Policy Committee and the Senate.

Section 30: Roles and Responsibilities

30.1 Purpose of This Section

This Section sets out the specific roles and responsibilities of different categories of University community members in relation to AI governance. These roles and responsibilities are binding on all members of the University community and shall be reflected in job descriptions, performance expectations, and disciplinary procedures where appropriate.

30.2 Senate

The Senate shall:

(a) Approve and amend this policy;

(b) Provide strategic oversight of AI governance;

(c) Receive and consider reports from the AI Policy Committee;

(d) Conduct periodic reviews of this policy;

(e) Approve major AI investments and initiatives;

(f) Ensure that AI adoption aligns with the University's mission and values.

30.3 Vice-Chancellor and Management

The Vice-Chancellor and University Management shall:

(a) Provide executive leadership for AI governance;

- (b) Ensure that adequate resources are allocated for AI implementation;
- (c) Appoint the Chairperson and members of the AI Policy Committee;
- (d) Receive regular reports on AI governance matters;
- (e) Represent the University in external AI-related engagements;
- (f) Ensure that AI governance is integrated into the University's strategic planning.

30.4 AI Policy Committee

The AI Policy Committee shall:

- (a) Oversee the implementation of this policy;
- (b) Develop guidance and procedures for AI governance;
- (c) Review and recommend AI tools and services;
- (d) Conduct and coordinate risk assessments;
- (e) Monitor compliance with this policy;
- (f) Prepare NUC compliance reports;
- (g) Coordinate AI training and awareness;
- (h) Maintain the AI system register;
- (i) Report annually to the Senate.

30.5 Deans and Heads of Department

Deans and Heads of Department shall:

- (a) Ensure that this policy is implemented within their Colleges and Departments;
- (b) Appoint College AI Representatives;
- (c) Ensure that course-level AI use statements are prepared and communicated to students;
- (d) Support staff in complying with this policy;
- (e) Report AI-related concerns to the AI Policy Committee;
- (f) Facilitate AI-related training and development within their units.

30.6 Academic Staff

Academic staff shall:

- (a) Comply with this policy in their teaching, research, and professional activities;
- (b) Include AI use statements in course syllabi;
- (c) Design AI-resilient assessments;
- (d) Model responsible AI use;
- (e) Provide clear guidance to students on AI use;

- (f) Report suspected AI-related misconduct;
- (g) Engage in professional development on AI;
- (h) Disclose AI use in their own research and professional work as required by this policy.

30.7 Administrative Staff

Administrative staff shall:

- (a) Comply with this policy in their administrative activities;
- (b) Use only approved AI tools for University-related work;
- (c) Exercise human oversight over AI-assisted decisions;
- (d) Protect personal data when using AI tools;
- (e) Report AI-related concerns and incidents;
- (f) Participate in AI training as required;
- (g) Maintain appropriate records of AI-assisted administrative decisions.

30.8 Students

Students shall:

- (a) Comply with this policy and with course-level AI use guidelines;
- (b) Use AI tools responsibly and ethically;
- (c) Disclose AI use as required by this policy;
- (d) Verify the accuracy of AI-generated content;
- (e) Not use AI to commit academic misconduct;
- (f) Report AI-related concerns to appropriate University authorities;
- (g) Respect the privacy and data protection rights of others when using AI;
- (h) Engage with AI literacy training and resources provided by the University.

30.9 ICT Staff

ICT staff shall:

- (a) Implement and maintain AI infrastructure and systems;
- (b) Ensure the security of AI systems;
- (c) Provide technical support for AI tools and services;
- (d) Monitor AI system performance and reliability;
- (e) Support incident response for AI-related security breaches;
- (f) Maintain the AI system register;
- (g) Participate in AI-related technical training.

30.10 Data Protection Officer

The DPO shall:

- (a) Advise on data protection compliance for AI systems;
- (b) Conduct and review DPIAs;
- (c) Handle data subject rights requests;
- (d) Monitor compliance with the NDPA and this policy;
- (e) Lead breach response for AI-related data breaches;
- (f) Maintain records of processing activities and DPIAs;
- (g) Deliver data protection training;
- (h) Report to the AI Policy Committee on data protection matters.

30.11 Library Staff

Library staff shall:

- (a) Curate and provide access to AI-related resources;
- (b) Provide research support for AI-related projects;
- (c) Deliver information literacy training with AI content;
- (d) Manage the institutional repository;
- (e) Support students and staff on AI-related information matters.

30.12 External Partners and Vendors

External partners and vendors shall:

- (a) Comply with this policy and applicable Nigerian law when engaging with the University on AI-related matters;
- (b) Enter into data processing agreements that comply with the NDPA;
- (c) Implement appropriate security measures for University data;
- (d) Cooperate with University audits and assessments;
- (e) Notify the University of any data breaches or security incidents;
- (f) Return or delete University data upon termination of agreements.

Section 31: Compliance and Monitoring**31.1 Foundational Position**

McPherson University affirms that the effectiveness of this policy depends on robust compliance and monitoring mechanisms. The NUC has committed to enforcing compliance with its AI policy framework through rigorous, periodic monitoring of individual university AI development using a standardised

reporting template. The University aligns fully with this expectation and shall implement internal compliance and monitoring mechanisms that meet or exceed NUC requirements.

31.2 Compliance Requirements for All University Members

All members of the University community shall:

- (a) **Comply with this policy.** Comply with all applicable provisions of this policy in their AI-related activities.
- (b) **Cooperate with monitoring.** Cooperate with monitoring, auditing, and assessment activities conducted under this policy.
- (c) **Report violations.** Report known or suspected violations of this policy to the appropriate University authority.
- (d) **Participate in training.** Participate in AI training and awareness programmes as required.
- (e) **Maintain records.** Maintain records of AI use as required by this policy and any applicable procedures.

31.3 Regular Monitoring of AI Use

The University shall implement regular monitoring of AI use across all Colleges and units. Monitoring shall include:

- (a) **System monitoring.** Technical monitoring of AI systems to ensure proper functioning, security, and compliance with configuration requirements.
- (b) **Usage monitoring.** Monitoring of AI tool usage patterns to identify potential compliance issues, security risks, or misuse.
- (c) **Compliance reviews.** Periodic reviews of compliance with this policy, including reviews of course-level AI use statements, disclosure forms, and risk assessments.
- (d) **Data protection monitoring.** Monitoring of compliance with data protection requirements, including DPIAs, consent management, and data subject rights.
- (e) **Incident monitoring.** Monitoring of AI-related incidents to identify patterns and emerging risks.

Monitoring shall be conducted in a manner that respects the privacy and rights of individuals, and in accordance with the NDPA.

31.4 Annual AI Policy Compliance Report to Senate

The AI Policy Committee shall prepare and submit an annual AI Policy Compliance Report to the Senate. The Report shall include:

- (a) **Implementation status.** An assessment of the implementation of this policy across the University.
- (b) **Compliance summary.** A summary of compliance with key provisions of this policy.
- (c) **AI system inventory.** An updated inventory of AI systems deployed at the University, including risk categorisations.
- (d) **Training and awareness.** A summary of AI training and awareness activities conducted during the reporting period.

(e) **Incidents and breaches.** A summary of AI-related incidents and data breaches, including responses and lessons learned.

(f) **Audit findings.** A summary of internal and external audit findings related to AI.

(g) **NUC reporting.** A summary of reports submitted to the NUC and any feedback received.

(h) **Challenges and recommendations.** An assessment of challenges encountered in implementing this policy and recommendations for improvement.

(i) **Emerging issues.** An overview of emerging AI developments and their implications for the University.

The Report shall be submitted to the Senate within three months of the end of each academic year.

31.5 Internal Audits of AI Systems and Practices

The University's Internal Audit Unit shall conduct periodic audits of AI systems and practices. These audits shall:

(a) **Assess compliance.** Assess compliance with this policy and applicable legal requirements.

(b) **Evaluate controls.** Evaluate the effectiveness of technical and organisational controls for AI systems.

(c) **Identify risks.** Identify risks and control weaknesses related to AI.

(d) **Make recommendations.** Make recommendations for improving AI governance and controls.

(e) **Report findings.** Report audit findings to the AI Policy Committee, the Vice-Chancellor, and the Senate as appropriate.

Internal audits shall be conducted at least annually for high-risk and critical-risk AI systems, and periodically for other AI systems.

31.6 NUC Compliance Monitoring Preparation

The University shall prepare for NUC compliance monitoring by:

(a) **Maintaining documentation.** Maintaining comprehensive documentation of AI policies, procedures, systems, and activities.

(b) **Preparing reports.** Preparing reports in the format required by the NUC, using the Commission's standardised reporting template.

(c) **Conducting self-assessments.** Conducting periodic self-assessments against the NUC's AI Policy Framework to identify gaps and areas for improvement.

(d) **Designating a contact point.** Designating a contact point for NUC communications on AI matters.

(e) **Responding to requests.** Responding promptly and fully to NUC requests for information and documentation.

(f) **Implementing recommendations.** Implementing recommendations from NUC monitoring visits and reports.

The AI Policy Committee shall be responsible for coordinating NUC compliance monitoring preparation.

31.7 Corrective Action for Non-Compliance

Where non-compliance with this policy is identified, the University shall take appropriate corrective action. Corrective action may include:

- (a) **Remedial guidance.** Providing guidance and support to address the non-compliance.
- (b) **Corrective plans.** Requiring the development and implementation of corrective action plans.
- (c) **Additional training.** Requiring additional training for individuals or units involved in non-compliance.
- (d) **System changes.** Requiring changes to AI systems or configurations to address non-compliance.
- (e) **Disciplinary action.** Taking disciplinary action against individuals who violate this policy, in accordance with the University's disciplinary procedures.
- (f) **Contractual remedies.** Pursuing contractual remedies against vendors or partners who fail to comply with their obligations.

Corrective action shall be proportionate to the nature and severity of the non-compliance and shall be designed to prevent recurrence.

31.8 Whistleblower Protections

The University affirms that individuals who report violations of this policy in good faith shall be protected from retaliation. The University's Whistleblower Policy shall apply to reports of AI-related violations. Protections shall include:

- (a) **Confidentiality.** Protection of the identity of whistleblowers to the extent permitted by law.
- (b) **Non-retaliation.** Prohibition of retaliation, discrimination, or adverse action against whistleblowers.
- (c) **Fair treatment.** Fair treatment of whistleblowers throughout the investigation and resolution process.
- (d) **Access to support.** Access to support and guidance for whistleblowers.

Section 32: Review and Amendment

32.1 Foundational Position

McPherson University recognises that AI governance is a dynamic field requiring regular review and adaptation. The NUC's AI Policy Framework emphasises the importance of annual Senate policy review cycles. This Section establishes the mechanisms for reviewing and amending this policy to ensure that it remains fit for purpose in a rapidly evolving technological and regulatory environment.

32.2 Scheduled Policy Review

The Senate shall conduct a comprehensive review of this policy at least every two years. The review shall consider:

- (a) **Effectiveness.** The effectiveness of the policy in achieving its objectives.
- (b) **Compliance.** The level of compliance with the policy across the University.
- (c) **Emerging developments.** Developments in AI technology, regulation, and best practice since the last review.

(d) **Stakeholder feedback.** Feedback from staff, students, and other stakeholders on the operation of the policy.

(e) **NUC guidance.** Any updated guidance or requirements from the NUC.

(f) **Legal developments.** Changes in Nigerian law or international standards relevant to AI governance.

(g) **Institutional experience.** Lessons learned from the implementation of the policy, including from incidents, audits, and compliance monitoring.

The AI Policy Committee shall prepare a review report for the Senate, including recommendations for amendments or continuation of the policy.

32.3 Triggers for Unscheduled Review

In addition to the scheduled biennial review, the Senate may initiate an unscheduled review of this policy in response to:

(a) **Significant AI developments.** Major technological developments that materially affect the University's AI governance.

(b) **Regulatory changes.** Changes in NUC guidance, Nigerian law, or international standards that require policy amendments.

(c) **Significant incidents.** AI-related incidents that reveal gaps or weaknesses in the policy.

(d) **Stakeholder concerns.** Significant concerns raised by staff, students, or other stakeholders.

(e) **Audit findings.** Audit findings that indicate the need for policy revision.

(f) **Institutional changes.** Changes in the University's structure, mission, or strategic priorities that affect AI governance.

32.4 Amendment Procedure

Amendments to this policy shall follow the procedure set out below:

(a) **Proposal.** Amendments may be proposed by the AI Policy Committee, the Vice-Chancellor, a Dean, or any member of the Senate.

(b) **Consultation.** Proposed amendments shall be circulated to relevant stakeholders for consultation, including the AI Policy Committee, the DPO, and, where appropriate, student and staff representatives.

(c) **Review.** The AI Policy Committee shall review proposed amendments and provide recommendations to the Senate.

(d) **Approval.** Amendments shall be approved by the Senate through its established procedures.

(e) **Effective date.** Amendments shall take effect from the date specified by the Senate.

(f) **Communication.** Approved amendments shall be communicated to the University community through the channels described in Section 27.

32.5 Version Control and Documentation

The University shall maintain proper version control and documentation for this policy. This shall include:

- (a) **Version numbering.** Each version of the policy shall be clearly numbered and dated.
- (b) **Change log.** A change log shall be maintained recording all amendments, the reasons for the changes, and the dates of approval and effect.
- (c) **Archival.** Previous versions of the policy shall be archived and made accessible for reference.
- (d) **Publication.** The current version of the policy shall be published on the University website.
- (e) **Retention.** Records of policy development, consultation, and approval shall be retained in accordance with the University's records retention policy.

32.6 Stakeholder Consultation in Review

The University shall consult with stakeholders as part of the policy review process. Consultation shall include:

- (a) **Staff consultation.** Consultation with academic and administrative staff through their representative bodies and through open consultation processes.
- (b) **Student consultation.** Consultation with students through the Student Representative Council and other student bodies.
- (c) **AI Policy Committee consultation.** Consultation with the AI Policy Committee and its subcommittees.
- (d) **External consultation.** Where appropriate, consultation with external experts, peer institutions, and regulatory bodies.
- (e) **Public consultation.** Where appropriate, public consultation on significant policy changes.

The University shall document consultation processes and shall consider stakeholder feedback in the review and amendment of this policy.

32.7 Alignment with National Review Cycles

The University shall align its policy review cycles with national AI governance developments, including:

- (a) **NUC review cycles.** Aligning with any NUC review cycles for AI policy frameworks.
- (b) **National AI Strategy review.** Aligning with reviews of the Nigeria National Artificial Intelligence Strategy.
- (c) **Legislative developments.** Monitoring and responding to legislative developments related to AI.
- (d) **Regulatory guidance.** Monitoring and responding to guidance from NITDA, NDPC, and other regulatory bodies.

The AI Policy Committee shall monitor national developments and shall advise the Senate on the timing and scope of policy reviews.

Part Ten: Implementation and Transition

Section 33: Implementation Plan

33.1 Foundational Position

McPherson University recognises that the adoption of a policy, however well designed, is only the beginning. The success of this Artificial Intelligence Policy will depend on the quality, coherence, and discipline of its implementation. The University further recognises that AI governance is not a one-time project but a continuous process of learning, adaptation, and improvement. As the NUC's Artificial Intelligence Policy Framework and Implementation Roadmap for the Nigerian University System has emphasised, responsible AI integration requires structured, sustained effort rather than episodic intervention.

The University notes the NUC's broader strategic direction, including the Draft National STEM Transformation Strategy for Higher Education in Nigeria (2026–2036), developed with support from the Agence Française de Développement's Blueprint ICT-Dev Project. That strategy provides a ten-year roadmap covering curriculum modernisation, digital infrastructure, faculty development, research commercialisation, quality assurance, and sustainable financing. This policy's implementation plan is designed to align with and contribute to that national strategy while remaining tailored to McPherson University's distinctive mission, scale, and resources.

The University adopts a phased implementation approach, recognising that different elements of this policy require different time horizons and resource commitments. The approach is informed by international best practice in higher education AI implementation, including the four-phase framework adopted by peer institutions such as Neumann University, which progressed through policy alignment and awareness, resource development and capacity building, framework and pilot implementation, and institutionalisation and visibility. The University's framework adapts this structure to its own context and priorities.

33.2 Phased Implementation Timeline

The University shall implement this policy over a period of thirty-six months, divided into four phases:

Phase One: Policy Adoption and Institutional Mobilisation (Months 1–6)

The first phase focuses on establishing the governance structures, operational foundations, and institutional awareness necessary for effective implementation. Key activities shall include:

- (a) **Senate approval and official adoption.** Formal adoption of this policy by the Senate and its communication to the University community.
- (b) **Establishment of the AI Policy Committee.** Constitution of the AI Policy Committee in accordance with Section 29.3, including appointment of the Chairperson and members, and convening of the Committee's inaugural meeting.
- (c) **Appointment of College AI Representatives.** Appointment of AI Representatives for each College in accordance with Section 29.4.
- (d) **Designation of the Data Protection Officer.** Confirmation of the University's DPO in accordance with Section 19.4, ensuring that the DPO has the authority and resources required to fulfil their responsibilities under this policy.

(e) **Baseline assessment.** Conduct of a comprehensive baseline assessment of the University's current AI use, AI-related capabilities, ICT infrastructure, and data governance practices.

(f) **Development of operational guidance.** Preparation and publication of operational guidance documents, including the five-category AI use scale, course-level syllabus statement templates, AI Use Disclosure Forms, and risk assessment methodologies.

(g) **Development of the AI System Register.** Establishment of the University's register of AI systems in accordance with Section 24.5.

(h) **Initial awareness campaign.** Launch of a University-wide awareness campaign to communicate the policy, explain its implications, and direct community members to resources and support.

The AI Policy Committee shall submit a Phase One completion report to the Senate within one month of the end of the phase.

Phase Two: Capacity Building and Tool Evaluation (Months 7–12)

The second phase focuses on building the University community's capacity for responsible AI use and on the systematic evaluation of AI tools and services. Key activities shall include:

(a) **AI literacy training for staff.** Delivery of baseline AI literacy training for all academic and administrative staff, in accordance with Section 26.

(b) **AI literacy integration for students.** Development and initiation of AI literacy content for students, including integration into existing courses and co-curricular activities.

(c) **Role-specific training.** Delivery of role-specific AI training for academic staff, administrative staff, ICT staff, library staff, and management staff, in accordance with Section 26.4.

(d) **AI tool evaluation and approval.** Systematic evaluation of AI tools and services for potential institutional adoption, including security, privacy, ethical, functional, and cost assessments in accordance with Section 25.

(e) **Establishment of approved AI tool list.** Publication of the University's initial list of approved AI tools and platforms.

(f) **Development of training resources.** Development and curation of AI training resources, including guides, case studies, and practical exercises, tailored to the University's context and disciplines.

(g) **Pilot programmes.** Initiation of pilot programmes for AI integration in teaching, learning, and administration, with rigorous evaluation and documentation of lessons learned.

(h) **AI capacity assessment.** Assessment of the University's progress in building AI capacity, including identification of remaining gaps and priorities for Phase Three.

The AI Policy Committee shall submit a Phase Two progress report to the Senate, including recommendations for adjustments to the implementation plan.

Phase Three: Integration and Scaling (Months 13–24)

The third phase focuses on scaling successful pilots, deepening AI integration across the University, and embedding AI governance into routine operations. Key activities shall include:

- (a) **Scaling successful pilots.** Expansion of successful AI pilot programmes to additional courses, departments, and administrative units.
- (b) **Curriculum integration.** Integration of AI literacy and ethics into the curriculum across all Colleges, in alignment with the CCMAS framework and the NUC's expectations for AI competency development.
- (c) **Advanced AI training.** Delivery of advanced AI training for staff who require deeper technical or disciplinary AI competence.
- (d) **Research capacity building.** Support for AI-related research through seed funding, research clusters, and collaboration facilitation, in accordance with Section 28.
- (e) **Infrastructure development.** Progressive development of AI-related ICT infrastructure, including computing resources, connectivity, and cloud arrangements, in accordance with the Infrastructure Development Roadmap (Section 22.8).
- (f) **Data governance implementation.** Full implementation of the data governance framework established in Sections 19 to 21, including DPIAs, audit trails, and retention schedules.
- (g) **External partnership development.** Development of partnerships with industry, government, and other institutions for AI-related collaboration, in accordance with Section 28.4.
- (h) **NUC compliance reporting.** Preparation and submission of the University's first comprehensive AI compliance report to the NUC using the Commission's standardised reporting template.

The AI Policy Committee shall submit a Phase Three report to the Senate, including an assessment of progress against the implementation plan and recommendations for Phase Four.

Phase Four: Institutionalisation and Continuous Improvement (Months 25–36)

The fourth phase focuses on embedding AI governance into the University's routine operations, culture, and strategic planning, and on establishing mechanisms for continuous improvement. Key activities shall include:

- (a) **Institutionalisation of AI governance.** Integration of AI governance into the University's routine committee structures, planning processes, and quality assurance mechanisms.
- (b) **First biennial policy review.** Conduct of the first comprehensive review of this policy in accordance with Section 32.2.
- (c) **Sustainability planning.** Development of sustainable funding and resource models for ongoing AI infrastructure, training, and governance.
- (d) **Expansion of AI research and innovation.** Further development of AI research capacity, including pursuit of external funding, publication, and knowledge dissemination.
- (e) **External visibility and engagement.** Raising the University's external profile in AI governance through publications, conference presentations, and engagement with national and international networks.
- (f) **Continuous improvement mechanisms.** Establishment of ongoing mechanisms for monitoring, evaluation, and improvement of AI governance, including feedback loops from staff, students, and external partners.
- (g) **Strategic integration.** Integration of AI governance into the University's next strategic planning cycle.

33.3 Immediate Priorities

The University recognises that certain actions are urgent and should commence immediately upon the effective date of this policy. These immediate priorities are:

- (a) **Constitution of the AI Policy Committee** within thirty days of the policy's effective date.
- (b) **Publication of the policy** on the University website and dissemination to all staff and students within fourteen days of Senate approval.
- (c) **Issuance of interim guidance** to academic staff on AI use in teaching and assessment, pending the development of full operational guidance.
- (d) **Communication to students** regarding the policy's key provisions and the availability of support resources.
- (e) **Initiation of the AI tool evaluation process** for tools already in use or immediately required by the University.
- (f) **Notification to the NUC** of the University's adoption of this policy, in accordance with the Commission's reporting expectations.

33.4 Resource Requirements and Budget

The implementation of this policy will require resources across several categories. The AI Policy Committee, in collaboration with the Bursary and the ICT Directorate, shall prepare a detailed implementation budget for consideration by the University Management and the Senate. The budget shall address:

- (a) **Personnel.** Staff time for AI governance activities, training delivery, and technical support; possible additional appointments or consultancy engagements for specialist AI expertise.
- (b) **Training and development.** Costs of AI training programmes, workshops, seminars, and professional development activities for staff and students.
- (c) **ICT infrastructure.** Costs of computing resources, connectivity upgrades, cloud services, and software licences for AI tools and platforms.
- (d) **Research support.** Seed funding for AI-related research, conference support, and publication costs.
- (e) **Compliance and auditing.** Costs of DPIAs, security assessments, internal audits, and external compliance reviews.
- (f) **Communication and awareness.** Costs of developing and disseminating awareness materials, including website development, publications, and events.
- (g) **Contingency.** A contingency allowance for unforeseen costs and emerging priorities.

The University shall prioritise resource allocation to activities with the highest impact on compliance, capacity building, and student learning. Where resources are constrained, the AI Policy Committee shall recommend phased or prioritised implementation.

33.5 Risk Mitigation During Transition

The University recognises that transitions to new governance frameworks can introduce risks, including resistance, confusion, resource strain, and unintended consequences. The University shall adopt the following risk mitigation measures during the implementation period:

- (a) **Clear communication.** Sustained, multi-channel communication about the policy, its rationale, and its implications, in accordance with Section 27.
- (b) **Stakeholder engagement.** Ongoing engagement with staff, students, and other stakeholders to identify concerns and adjust implementation approaches.
- (c) **Gradual compliance.** A grace period for compliance with new requirements, particularly for academic staff adjusting course design and assessment practices.
- (d) **Support and resources.** Provision of adequate support and resources to enable compliance, including training, guidance, and technical assistance.
- (e) **Monitoring and adjustment.** Regular monitoring of implementation progress and adjustment of the implementation plan in response to emerging challenges.
- (f) **Leadership visibility.** Visible leadership commitment to the policy, including from the Vice-Chancellor, Deans, and other senior officers.

The University notes the experience of institutions such as Indiana University's Kelley School of Business, which found that rigid, policy-heavy approaches were less effective than lean, values-based frameworks supported by visible leadership, sustained communication, and practical resources. The University shall adopt a similarly adaptive and supportive approach, emphasising experimentation, curiosity, and continuous learning rather than immediate mastery.

Section 34: Resource Mobilisation

34.1 Foundational Position

McPherson University recognises that the successful implementation of this policy requires adequate and sustainable resources. The University further recognises that resources for AI governance and adoption must be mobilised from multiple sources, including internal budget allocation, external funding, partnerships, and cost-sharing arrangements. This Section sets out the University's approach to resource mobilisation.

The University notes that Nigerian universities are actively pursuing external funding for AI-related initiatives. TETFund has approved ₦3 billion special intervention grants for the establishment of AI Centres of Excellence at Lagos State University and Federal University Lokoja under the 2026 Special Intervention Projects allocation. These grants demonstrate the availability of national funding for university AI initiatives and provide a model that McPherson University shall seek to replicate, adapted to its private university context.

34.2 Budget Allocation for AI Infrastructure and Training

The University shall allocate resources in its annual budget for AI-related activities. Budget allocation shall cover:

- (a) **Recurring costs.** Ongoing costs of AI tools, subscriptions, cloud services, and maintenance of AI infrastructure.
- (b) **Capital costs.** Acquisition of computing resources, networking equipment, and other AI-related capital assets.
- (c) **Training costs.** Delivery of AI training programmes, workshops, and professional development activities.
- (d) **Research support.** Funding for AI-related research, including seed grants and conference support.
- (e) **Compliance costs.** Costs of DPIAs, audits, security assessments, and other compliance activities.

The Bursary, in collaboration with the AI Policy Committee and the ICT Directorate, shall prepare annual budget proposals for AI-related activities and shall present them to Management and the Senate for approval.

34.3 Internal Resource Reallocation

Where external funding is limited, the University shall consider internal resource reallocation to support AI priorities. This may include:

- (a) **Prioritisation within existing budgets.** Identifying opportunities to redirect existing budgets toward AI-related priorities.
- (b) **Efficiency savings.** Using AI to generate efficiency savings that can be reinvested in AI governance and capacity building.
- (c) **Cost-sharing between units.** Encouraging units to share the costs of AI tools, infrastructure, and training.
- (d) **Phased investment.** Investing in AI capabilities in phases, prioritising foundational infrastructure and capacity building before advanced applications.

The University shall ensure that resource reallocation does not compromise other essential functions and shall consult with affected units before making significant reallocations.

34.4 External Funding Opportunities

The University shall actively pursue external funding opportunities for AI-related activities. These shall include:

- (a) **TETFund intervention.** The University shall explore eligibility for TETFund special intervention projects, including AI-related infrastructure, research, and capacity-building initiatives.
- (b) **Government programmes.** The University shall engage with government programmes that support AI development in higher education, including those administered by NITDA, the Federal Ministry of Communications, Innovation and Digital Economy, and other relevant agencies.
- (c) **International development partners.** The University shall explore funding opportunities from international development partners, including UNESCO, the African Development Bank, the Agence Française de Développement, and other organisations supporting AI capacity building in African higher education.

(d) **Private foundations and philanthropy.** The University shall engage with private foundations and philanthropic organisations that support higher education, technology, and AI-related initiatives.

(e) **Corporate partnerships.** The University shall explore corporate partnerships, including with technology companies such as Google, which has committed \$1.1 million to AI training at ten Nigerian universities through the Africa AI Upskilling Programme, and MTN, with which the University has already engaged on data centre and cloud infrastructure matters.

(f) **Research grants.** The University shall support staff in applying for research grants from national and international funders for AI-related research.

The Research Office, in collaboration with the AI Policy Committee and the University's Development Office, shall coordinate the pursuit of external funding opportunities.

34.5 Industry Collaboration and Sponsorship

The University shall develop industry collaboration and sponsorship arrangements to support AI-related activities. These may include:

(a) **Corporate sponsorship.** Sponsorship of AI infrastructure, training programmes, or research initiatives by industry partners.

(b) **In-kind contributions.** In-kind contributions of technology, expertise, or services by industry partners.

(c) **Joint ventures.** Joint ventures with industry partners for AI-related research, development, or commercialisation.

(d) **Advisory support.** Industry advisory support for AI curriculum development, training design, and research priorities.

(e) **Internship and placement.** Industry partnerships for student internships and graduate placement in AI-related roles.

The University shall ensure that industry collaborations are governed by written agreements that address intellectual property, data protection, and alignment with the University's mission and values.

34.6 Cost-Sharing Mechanisms

The University shall explore cost-sharing mechanisms to distribute the financial burden of AI adoption. These may include:

(a) **Shared services.** Sharing AI tools and infrastructure across Colleges and units to reduce duplication and costs.

(b) **Consortium arrangements.** Collaborating with other universities or institutions on shared AI resources, training, and research.

(c) **User contributions.** Where appropriate, modest user contributions for certain AI services, with provisions for financial hardship.

(d) **Graduate assistant support.** Using graduate assistants to support AI-related teaching, research, and administrative tasks.

The University shall ensure that cost-sharing mechanisms do not create inequities or barriers to access for students or staff.

34.7 Sustainability Planning

The University shall develop sustainability plans for AI-related activities, ensuring that funding is not only secured for initial implementation but also for ongoing operations. Sustainability planning shall address:

- (a) **Recurring funding.** Securing recurring funding for AI tools, infrastructure, and personnel.
- (b) **Revenue generation.** Exploring opportunities for revenue generation through AI-related services, training, or consultancy.
- (c) **Cost optimisation.** Continuously optimising AI-related costs through efficient procurement, shared services, and technology choices.
- (d) **Capacity retention.** Ensuring that the University retains the staff expertise needed to manage AI systems and governance over the long term.
- (e) **Institutional commitment.** Embedding AI-related expenditure in the University's core budget rather than relying solely on project-based or donor funding.

The AI Policy Committee shall review sustainability arrangements annually and shall report to the Senate on the financial sustainability of AI-related activities.

Section 35: Stakeholder Engagement

35.1 Foundational Position

McPherson University affirms that effective AI governance requires the engagement of all stakeholders who are affected by AI-related decisions and practices. The University notes that research on AI governance in higher education has emphasised the importance of inclusive governance structures that engage academia, civil society, and students, and that institutions should establish ongoing dialogue with students, faculty, and policymakers to ensure AI policies remain relevant and aligned with the needs of the academic community.

The University's stakeholder engagement approach is guided by the principle that AI governance is a shared responsibility. It is not the exclusive domain of management, ICT staff, or any single group. All members of the University community have a stake in ensuring that AI is used responsibly, and all should have opportunities to contribute to the development and implementation of AI governance.

35.2 Senate and Management Consultation

The Senate and University Management are the primary institutional stakeholders for AI governance. Consultation with these bodies shall occur through:

- (a) **Senate approval and oversight.** Formal Senate approval of this policy and ongoing Senate oversight of its implementation, as provided in Sections 29.2 and 31.4.
- (b) **Management briefings.** Regular briefings to Management on AI-related developments, challenges, and progress.

(c) **Committee reports.** Reports from the AI Policy Committee to the Senate and Management as provided in Section 29.3.

(d) **Strategic planning.** Integration of AI governance into the University's strategic planning processes.

35.3 Faculty and Staff Consultation

Faculty and staff are essential partners in AI governance. Consultation with faculty and staff shall occur through:

(a) **Staff representative bodies.** Engagement with academic and non-academic staff associations and unions on AI-related matters.

(b) **Departmental consultations.** Consultations with Colleges and Departments on AI policies, tools, and practices.

(c) **Survey mechanisms.** Periodic surveys to assess staff attitudes, concerns, and needs regarding AI.

(d) **Open forums.** Periodic open forums where staff can raise questions, share experiences, and contribute to AI governance discussions.

(e) **Committee representation.** Staff representation on the AI Policy Committee and its subcommittees, as provided in Section 29.3.

The University notes the importance of engaging the "movable middle" of faculty and staff who are open to AI adoption but may lack the confidence, skills, or resources to engage effectively. Engagement efforts shall therefore prioritise practical support, training, and resources rather than attempting to persuade the resistant or merely affirm the already committed.

35.4 Student Consultation

Students are the primary beneficiaries of the University's educational mission and are directly affected by AI-related policies and practices. Consultation with students shall occur through:

(a) **Student representative bodies.** Engagement with the Student Representative Council and other student organisations on AI-related matters.

(b) **Student representation on committees.** Student representation on the AI Policy Committee, as provided in Section 29.3.

(c) **Student surveys.** Periodic surveys to assess student attitudes, concerns, and experiences with AI.

(d) **Student forums.** Periodic forums where students can raise concerns, ask questions, and contribute to AI governance discussions.

(e) **Feedback mechanisms.** Accessible channels for students to provide feedback on AI policies, tools, and practices.

The University affirms the importance of student agency in AI governance. Students are not merely passive recipients of AI policies; they are active participants in the learning process and should have meaningful opportunities to shape the AI environment in which they learn.

35.5 Alumni and Community Engagement

The University shall engage with its alumni and the broader community on AI-related matters. This shall include:

- (a) **Alumni networks.** Engagement with alumni networks to share AI developments, seek expertise, and facilitate mentorship and collaboration.
- (b) **Community engagement.** Engagement with the local community on AI-related issues, including through public lectures, workshops, and community service.
- (c) **Alumni expertise.** Leveraging alumni expertise in AI and related fields to support the University's AI governance and capacity building.

35.6 Industry and Professional Body Engagement

The University shall engage with industry and professional bodies on AI-related matters. This shall include:

- (a) **Industry advisory input.** Seeking industry input on AI curriculum design, training needs, and research priorities.
- (b) **Professional body engagement.** Engagement with professional bodies relevant to the University's programmes, including those in health, law, computing, and business, on AI-related standards and practices.
- (c) **Industry partnerships.** Development of partnerships with industry for AI-related research, training, and student placement.

35.7 Regulatory Agency Engagement

The University shall engage with regulatory agencies on AI-related matters. This shall include:

- (a) **NUC engagement.** Regular engagement with the NUC on AI policy compliance, reporting, and capacity building, in accordance with the NUC's AI Policy Framework and monitoring requirements.
- (b) **NITDA engagement.** Engagement with the National Information Technology Development Agency on AI-related standards, guidance, and initiatives.
- (c) **NDPC engagement.** Engagement with the Nigeria Data Protection Commission on data protection matters related to AI, including compliance with the NDPA and the GAID.
- (d) **Other agencies.** Engagement with other relevant regulatory agencies as required.

35.8 International Partner Engagement

The University shall engage with international partners on AI-related matters. This shall include:

- (a) **International networks.** Participation in international networks focused on AI in higher education, including UNESCO's AI in Education initiatives and the IIOE network.
- (b) **International partnerships.** Development of partnerships with international institutions for AI research, capacity building, and knowledge exchange.
- (c) **International standards.** Engagement with the development and adoption of international AI standards and best practices.

35.9 Engagement Mechanisms and Feedback Loops

The University shall establish mechanisms to ensure that stakeholder engagement informs decision-making and that stakeholders receive feedback on how their input has been used. These mechanisms shall include:

- (a) **Consultation reports.** Preparation of reports summarising stakeholder input and how it has been considered.
- (b) **Feedback communication.** Communication to stakeholders on decisions made and the reasons for those decisions.
- (c) **Ongoing dialogue.** Establishment of ongoing dialogue mechanisms, including regular meetings, forums, and communications.
- (d) **Evaluation.** Periodic evaluation of stakeholder engagement effectiveness and adjustment of engagement approaches as needed.

Section 36: Policy Launch and Communication

36.1 Foundational Position

McPherson University recognises that the successful launch of this policy depends on effective communication. The University notes the experience of institutions such as Indiana University's Kelley School of Business, which found that AI communication strategies should be anchored around values and identity rather than the technology itself, and that sustained, multichannel communications and visible actions are essential for building momentum. The University further notes that institutions should emphasise experimentation, curiosity, and continuous learning rather than mastery from day one.

The University's approach to policy launch and communication is therefore designed to be values-anchored, sustained, multi-channel, and supportive. It is not a one-time event but an ongoing process of engagement.

36.2 Official Launch and Dissemination

The University shall officially launch this policy through a series of coordinated activities:

- (a) **Senate approval and announcement.** Formal Senate approval of the policy and public announcement of its adoption.
- (b) **Launch event.** A launch event bringing together staff, students, and stakeholders to introduce the policy and explain its significance.
- (c) **Website publication.** Immediate publication of the policy on the University website in an accessible format.
- (d) **Email dissemination.** Direct email communication to all staff and students announcing the policy and providing links to the full document and supporting resources.
- (e) **Physical distribution.** Distribution of printed copies or summaries to Colleges, Departments, and administrative units.
- (f) **Media engagement.** Engagement with University media and, where appropriate, external media to communicate the policy's adoption.

36.3 Website Publication and Accessibility

The University shall ensure that this policy is published on the University website in a manner that is:

- (a) **Accessible.** Available to all users, including persons with disabilities, in accessible formats.
- (b) **Discoverable.** Easily found through the University's website navigation and search functions.
- (c) **Contextualised.** Accompanied by supporting resources, including FAQs, training materials, and contact information.
- (d) **Current.** Regularly updated to reflect amendments and new guidance.
- (e) **Archived.** Historical versions maintained for reference and accountability.

The University notes that the public availability of its AI policy and related documentation contributes to institutional transparency and may be considered in NUC ranking assessments. The University shall therefore ensure that its published AI materials present the University's AI governance framework clearly and professionally.

36.4 Orientation Sessions

The University shall conduct orientation sessions for different stakeholder groups:

- (a) **Staff orientation.** Sessions for academic and administrative staff introducing the policy, explaining its implications for their work, and providing practical guidance.
- (b) **Student orientation.** Sessions for students introducing the policy, explaining their responsibilities and rights, and providing guidance on responsible AI use.
- (c) **Management orientation.** Sessions for Management and senior officers on their leadership responsibilities under the policy.
- (d) **Departmental briefings.** Briefings conducted by Deans and Heads of Department for their units, supported by materials and guidance from the AI Policy Committee.

Orientation sessions shall be conducted within three months of the policy's effective date and shall be repeated periodically for new staff and students.

36.5 Integration with Student and Staff Handbooks

The University shall integrate this policy into the Student Handbook and Staff Handbook, ensuring that:

- (a) **Key provisions are summarised.** Key provisions of the policy, including AI use categories, disclosure requirements, and disciplinary consequences, are summarised in accessible language.
- (b) **Cross-references are included.** References to the full policy and supporting resources are included.
- (c) **Updates are maintained.** Handbook content is updated as the policy is amended.
- (d) **Accessibility is ensured.** Handbook content is accessible to all staff and students, including those with disabilities.

36.6 NUC Notification and Ranking Documentation

The University shall notify the NUC of its adoption of this policy and shall provide documentation as required by the Commission's AI Policy Framework and monitoring processes. This shall include:

- (a) **Formal notification.** Written notification to the NUC of the policy's adoption, including a summary of key provisions.
- (b) **Policy submission.** Submission of the full policy document to the NUC for its records.
- (c) **Compliance documentation.** Documentation demonstrating the University's compliance with the NUC's AI Policy Framework and Implementation Roadmap.
- (d) **Ranking documentation.** Inclusion of the policy and related documentation in materials submitted for NUC ranking assessments.

The AI Policy Committee, in collaboration with the Vice-Chancellor's Office, shall coordinate NUC notification and reporting.

36.7 Communication Strategy Principles

The University's communication strategy for this policy shall be guided by the following principles:

- (a) **Values-anchored.** Communications shall emphasise the University's mission, vision, and values, and shall explain how AI governance serves those commitments.
- (b) **Sustained and multi-channel.** Communications shall be ongoing and shall use multiple channels, including email, website, social media, physical notices, and face-to-face engagement.
- (c) **Supportive.** Communications shall emphasise support, resources, and guidance rather than enforcement and punishment.
- (d) **Practical.** Communications shall provide practical guidance and examples relevant to different stakeholder groups.
- (e) **Adaptive.** Communications shall be adjusted based on feedback and emerging needs.
- (f) **Transparent.** Communications shall be honest about challenges, uncertainties, and the evolving nature of AI governance.

36.8 First-Year Communication Priorities

During the first year of implementation, the University's communication priorities shall be:

- (a) **Awareness.** Ensuring that all staff and students are aware of the policy, its key provisions, and available support.
- (b) **Understanding.** Building understanding of the policy's rationale, requirements, and implications.
- (c) **Engagement.** Encouraging staff and student engagement with AI governance, including through feedback, consultation, and participation in training.
- (d) **Support.** Ensuring that staff and students know where to access support, guidance, and resources.
- (e) **Trust.** Building trust in the University's approach to AI governance through transparency, consistency, and visible leadership commitment.

36.9 Measuring Communication Effectiveness

The University shall measure the effectiveness of its communication strategy through:

- (a) **Awareness surveys.** Periodic surveys to assess awareness of the policy among staff and students.
- (b) **Engagement metrics.** Tracking of participation in training, forums, and consultation activities.
- (c) **Feedback analysis.** Analysis of feedback received through various channels to identify communication gaps and improvement opportunities.
- (d) **Compliance indicators.** Monitoring of compliance with key provisions as an indicator of communication effectiveness.
- (e) **Continuous improvement.** Adjustment of communication approaches based on measurement results and stakeholder feedback.

The AI Policy Committee shall report to the Senate on communication effectiveness as part of its annual AI Policy Compliance Report.

Part Eleven: Miscellaneous and Supplementary Provisions

Section 37: Relationship to Other University Policies

37.1 Foundational Position

McPherson University recognises that this Artificial Intelligence Policy does not exist in isolation. It operates alongside, and must be read in conjunction with, the University's existing body of policies, regulations, and procedures. This Section clarifies the relationship between this policy and other University instruments, and establishes principles for resolving any conflicts or ambiguities that may arise.

The University affirms that this policy is intended to supplement, not supplant, existing policies. Where existing policies address AI-related matters, this policy provides additional specificity and governance. Where existing policies are silent on AI-related matters, this policy fills the gap. Where conflicts arise, the resolution principles in Section 37.9 shall apply.

37.2 Academic Integrity Policy

McPherson University's Academic Integrity Policy (FAC 604) establishes the University's expectations for academic honesty and the procedures for addressing academic dishonesty, including cheating, fabrication, and plagiarism. This AI Policy builds upon that foundation by:

- (a) **Extending definitions.** Clarifying how AI-related conduct falls within the existing categories of cheating, fabrication, and plagiarism;
- (b) **Providing AI-specific procedures.** Establishing the five-category AI use scale, disclosure requirements, and AI-specific misconduct procedures detailed in Sections 8 and 9;
- (c) **Preserving existing processes.** Ensuring that AI-related misconduct is investigated and adjudicated through the University's established academic dishonesty procedures, including the Academic Dishonesty Incident Report process and the student's right of appeal;
- (d) **Maintaining penalties.** Confirming that the existing penalty structure for academic dishonesty (including course failure, suspension, and dismissal for repeat offences) applies to AI-related misconduct.

Where a provision of this AI Policy conflicts with the Academic Integrity Policy on a matter relating specifically to AI, this policy shall prevail.

37.3 ICT Acceptable Use Policy

McPherson University's Information Technology Usage Policy (ADM 280) establishes the acceptable use of University computing and network resources, including prohibitions on unauthorised access, copyright infringement, and disruptive activities. This AI Policy builds upon that foundation by:

- (a) **Extending acceptable use principles.** Applying the existing principles of legal and ethical use, respect for intellectual property, and privacy protection to AI tools and systems;
- (b) **Adding AI-specific requirements.** Establishing additional requirements for AI tool approval, data protection in AI use, and human oversight of AI-assisted decisions;
- (c) **Clarifying prohibitions.** Explicitly prohibiting the use of AI for malicious purposes, including the generation of malware, deepfakes, and automated harassment, as detailed in Section 23.7;

(d) **Aligning sanctions.** Ensuring that violations of AI-related ICT requirements are subject to the same range of sanctions as other ICT policy violations, up to and including termination or expulsion.

Where a provision of this AI Policy conflicts with the ICT Acceptable Use Policy on a matter relating specifically to AI, this policy shall prevail.

37.4 Research Ethics Policy

McPherson University has demonstrated its commitment to research ethics through its attainment of National Health Research Ethics Committee (NHREC) certification, marking a significant milestone in the institution's commitment to ethical standards in health research and academic excellence. The University's Institutional Review Board guidelines establish requirements for the ethical review of research involving human subjects, sensitive topics, and innovative methodologies.

This AI Policy builds upon that foundation by:

(a) **Extending ethical review.** Requiring ethical review for AI-related research that involves human participants, personal data, or potential harm, as detailed in Section 13.1;

(b) **Adding AI-specific safeguards.** Establishing requirements for algorithmic bias assessment, data sovereignty, and the protection of human subjects in AI research;

(c) **Aligning with existing processes.** Ensuring that AI-related research is reviewed through the University's existing Research Ethics Committee processes, with the addition of AI-specific expertise where required;

(d) **Preserving research integrity.** Reinforcing the University's commitment to research integrity by prohibiting AI-related research misconduct, including fabrication, falsification, and plagiarism.

Where a provision of this AI Policy conflicts with the Research Ethics Policy on a matter relating specifically to AI, this policy shall prevail.

37.5 Data Protection Policy

McPherson University recognises that the Nigeria Data Protection Act 2023 (NDPA) and its General Application and Implementation Directive 2025 (GAID) establish comprehensive legal requirements for the processing of personal data. This AI Policy incorporates and builds upon those requirements by:

(a) **Operationalising NDPA requirements.** Translating the NDPA's principles into AI-specific operational requirements, including DPIAs, consent management, and data subject rights facilitation, as detailed in Section 19;

(b) **Addressing AI-specific data protection issues.** Establishing requirements for automated decision-making, algorithmic transparency, and data governance for AI systems;

(c) **Aligning with NDPC guidance.** Ensuring compliance with the Nigeria Data Protection Commission's guidance on emerging technologies, including AI;

(d) **Preserving existing rights.** Confirming that data subjects retain all rights under the NDPA, including the right not to be subjected to solely automated decisions with legal or similarly significant effects, as detailed in Section 19.8.

Where a provision of this AI Policy conflicts with the Data Protection Policy on a matter relating specifically to AI, this policy shall prevail. However, nothing in this policy shall be construed as limiting the rights of data subjects under the NDPA.

37.6 Human Resources Policy

McPherson University's Human Resources Policy governs the recruitment, management, development, and discipline of staff. This AI Policy builds upon that foundation by:

- (a) **Addressing AI in recruitment.** Establishing requirements for the use of AI in recruitment and selection processes, including human decision-making, transparency, and bias monitoring, as detailed in Section 18.1;
- (b) **Addressing AI in performance management.** Establishing requirements for the use of AI in performance management, including human judgment, fairness, and appeals, as detailed in Section 18.2;
- (c) **Addressing AI-related workforce changes.** Committing to transparent communication, reskilling opportunities, and fair treatment in relation to AI-related job displacement, as detailed in Section 18.5;
- (d) **Protecting staff data.** Ensuring that staff personal data processed by AI systems is protected in accordance with the NDPA, as detailed in Section 18.4.

Where a provision of this AI Policy conflicts with the Human Resources Policy on a matter relating specifically to AI, this policy shall prevail, subject to any applicable labour law requirements.

37.7 Student Handbook

The Student Handbook establishes the rights, responsibilities, and code of conduct for McPherson University students. This AI Policy shall be integrated into the Student Handbook, ensuring that:

- (a) **Key provisions are summarised.** Students have accessible information about AI use categories, disclosure requirements, and disciplinary consequences;
- (b) **Responsibilities are clear.** Students understand their responsibilities in relation to AI use, including the obligation to comply with course-level AI guidelines and to disclose AI use where required;
- (c) **Support is available.** Students know where to access support, guidance, and resources for responsible AI use;
- (d) **Rights are preserved.** Students' rights, including the right to appeal AI-related disciplinary decisions, are clearly stated.

37.8 Staff Handbook

The Staff Handbook establishes the terms and conditions of employment and the expectations for staff conduct at McPherson University. This AI Policy shall be integrated into the Staff Handbook, ensuring that:

- (a) **Responsibilities are clear.** Staff understand their responsibilities under this policy, including the obligation to use AI responsibly, to exercise human oversight over AI-assisted decisions, and to report AI-related concerns;
- (b) **Training expectations are stated.** Staff understand the AI training and development expectations applicable to their roles;

(c) **Disciplinary consequences are clear.** Staff understand that violations of this policy may result in disciplinary action;

(d) **Support is available.** Staff know where to access support, guidance, and resources for responsible AI use.

37.9 Conflict Resolution Between Policies

Where a conflict arises between this policy and another University policy on a matter relating to AI, the following principles shall apply:

(a) **Specificity.** The more specific provision shall prevail over the more general provision;

(b) **AI-specific provisions.** Where this policy contains a provision specifically addressing an AI-related matter, that provision shall prevail over a general provision in another policy;

(c) **Legal requirements.** Where a conflict arises between this policy and a legal requirement (including the NDPA, the Cybercrimes (Amendment) Act 2024, or other applicable law), the legal requirement shall prevail;

(d) **Mission alignment.** Where ambiguity remains, the interpretation most consistent with the University's mission, vision, and values shall be preferred;

(e) **Senate determination.** Where a conflict cannot be resolved through the above principles, the matter shall be referred to the Senate for determination.

The AI Policy Committee shall maintain a register of any identified conflicts or ambiguities and shall recommend amendments to the Senate as required.

Section 38: Legal Compliance and Liability

38.1 Foundational Position

McPherson University affirms its commitment to full compliance with all applicable Nigerian laws and regulations in relation to AI. The University further recognises that AI introduces novel legal questions regarding liability, indemnification, and dispute resolution. This Section establishes the University's approach to these matters.

38.2 Compliance with Nigerian Law

The University shall comply with all applicable Nigerian laws and regulations relating to AI, including:

(a) **The Nigeria Data Protection Act 2023** and its General Application and Implementation Directive 2025, as detailed in Section 19;

(b) **The Cybercrimes (Amendment) Act 2024**, as detailed in Section 23.6;

(c) **The Nigeria National Artificial Intelligence Strategy 2025–2029**, as detailed in Section 6.3;

(d) **NUC regulatory guidance**, including the NUC Artificial Intelligence Policy Framework and Implementation Roadmap, as detailed in Section 6.1;

(e) **NITDA guidelines and standards** on AI and emerging technologies;

(f) **Other applicable laws and regulations**, including labour law, consumer protection law, and intellectual property law.

The University shall monitor legal and regulatory developments and shall update this policy as required to maintain compliance.

38.3 Liability for AI-Related Harm

The University recognises that AI-related harm may arise from various sources, including:

- (a) **AI system failures.** Errors, malfunctions, or unexpected behaviour of AI systems;
- (b) **AI-generated content.** Harmful or misleading content generated by AI systems;
- (c) **AI-assisted decisions.** Decisions supported by AI that result in harm;
- (d) **AI-related data breaches.** Unauthorised access to or disclosure of personal data processed by AI systems;
- (e) **AI-related cyberattacks.** Attacks facilitated by or targeting AI systems.

Liability for AI-related harm shall be determined in accordance with applicable law and, where applicable, contractual arrangements with vendors and service providers. The University shall take reasonable steps to mitigate AI-related risks and shall maintain appropriate insurance coverage where feasible.

38.4 Indemnification and Insurance

- (a) **Vendor indemnification.** Contracts with AI vendors and service providers shall include appropriate indemnification provisions for AI-related losses, as detailed in Section 15.6;
- (b) **Insurance coverage.** The University shall review its insurance policies to determine whether they cover AI-related risks and shall consider additional coverage where appropriate, as detailed in Section 24.7;
- (c) **Staff indemnification.** The University shall consider whether and to what extent staff should be indemnified for AI-related liabilities arising from the good-faith performance of their duties;
- (d) **Student liability.** Students shall be liable for AI-related harm caused by their violation of this policy or other University policies, in accordance with the University's disciplinary procedures and applicable law.

38.5 Dispute Resolution

Disputes relating to AI use at McPherson University shall be resolved through the University's established dispute resolution procedures, including:

- (a) **Academic appeals.** Disputes relating to AI-related academic decisions shall be resolved through the University's academic appeals procedures;
- (b) **Grievance procedures.** Disputes relating to AI-related employment matters shall be resolved through the University's staff grievance procedures;
- (c) **Student complaints.** Disputes relating to AI-related student matters shall be resolved through the University's student complaints procedures;
- (d) **Mediation.** Where appropriate, disputes may be referred to mediation;

(e) **Arbitration or litigation.** Where internal resolution is not possible, disputes may be referred to arbitration or litigation in accordance with applicable law and contractual arrangements.

38.6 Governing Law

This policy shall be governed by and construed in accordance with the laws of the Federal Republic of Nigeria. Any legal proceedings relating to this policy shall be brought in the courts of competent jurisdiction in Nigeria.

Section 39: Special Provisions for Specific Programmes

39.1 Foundational Position

McPherson University recognises that different academic disciplines engage with AI in different ways, and that the governance requirements for AI use may vary across programmes. This Section establishes special provisions for specific programmes, recognising the distinctive characteristics of different fields of study.

These provisions are supplementary to, and do not replace, the general provisions of this policy. Where a special provision is more permissive than the general policy, the special provision shall prevail for that programme. Where a special provision is more restrictive, the more restrictive provision shall apply.

39.2 College of Computing

The College of Computing at McPherson University encompasses programmes in Computer Science, Information Technology, Software Engineering, Cyber Security, and Data Science. Given the technical nature of these programmes, the following special provisions apply:

- (a) **Advanced AI use.** Students and staff in the College of Computing may use AI tools at advanced levels, including for software development, algorithm design, and system architecture, subject to disclosure requirements appropriate to the context.
- (b) **AI system development.** Research and coursework involving the development of AI systems shall comply with the ethical requirements of this policy, including bias assessment, transparency, and human oversight.
- (c) **Professional standards.** Students and staff shall comply with the professional standards of the Computer Professionals Registration Council of Nigeria (CPRN) and other relevant professional bodies, including standards relating to data privacy, cybersecurity, and ethical practice.
- (d) **AI literacy leadership.** The College of Computing shall serve as a resource for AI literacy across the University, providing expertise, training, and support to other Colleges.

39.3 College of Allied Health Sciences

The College of Allied Health Sciences encompasses programmes in Nursing Science, Public Health, Medical Laboratory Science, and related fields. Given the sensitive nature of health data and the potential for AI to affect patient care, the following special provisions apply:

- (a) **Clinical AI use.** Students and staff in clinical settings shall use AI tools in accordance with clinical governance requirements, professional standards, and patient safety protocols.

(b) **Health data protection.** AI processing of patient data shall comply with the NDPA's requirements for sensitive personal data, including explicit consent and enhanced security measures.

(c) **Ethical review.** AI-related research involving human subjects shall be reviewed by the University's Research Ethics Committee, which has been strengthened by the University's NHREC certification.

(d) **Professional standards.** Students and staff shall comply with the professional standards of the Nursing and Midwifery Council of Nigeria, the Medical Laboratory Science Council of Nigeria, and other relevant regulatory bodies.

39.4 College of Law

The College of Law at McPherson University prepares students for legal practice, judicial service, and legal scholarship. Given the unique ethical and professional requirements of the legal profession, the following special provisions apply:

(a) **Legal research AI use.** Students and staff may use AI tools for legal research, document review, and drafting support, subject to verification of accuracy and compliance with professional conduct rules.

(b) **Client confidentiality.** AI processing of client information shall comply with legal professional privilege and confidentiality requirements.

(c) **Professional responsibility.** Students and staff shall comply with the Rules of Professional Conduct for Legal Practitioners in Nigeria, including rules relating to competence, confidentiality, and conflicts of interest.

(d) **AI and access to justice.** The College of Law shall explore the potential of AI to enhance access to justice, including through legal aid, community legal education, and legal technology innovation.

39.5 College of Natural and Applied Sciences

The College of Natural and Applied Sciences encompasses programmes in Biochemistry, Biotechnology, Microbiology, Industrial Chemistry, Industrial Mathematics, Medical Physics, and Statistics. Given the research-intensive nature of these programmes, the following special provisions apply:

(a) **Laboratory and field research.** AI tools may be used in laboratory and field research, including for data collection, analysis, and modelling, subject to the disclosure requirements in Section 12.

(b) **Data integrity.** AI-generated or AI-processed research data shall be validated and documented to ensure reproducibility and integrity.

(c) **Collaborative research.** AI-related research collaborations with external partners shall comply with the requirements of Section 13.6.

(d) **Publication ethics.** AI use in research publications shall comply with the disclosure requirements in Section 12.4 and any applicable journal or funder requirements.

39.6 College of Humanities, Social and Management Sciences

The College of Humanities, Social and Management Sciences encompasses programmes in Accounting, Business Administration, Economics, English, History and International Studies, Mass Communication, Political Science, and Sociology. Given the diverse nature of these programmes, the following special provisions apply:

- (a) **Writing-intensive courses.** In writing-intensive courses, AI use for language editing, structuring, and brainstorming is generally permitted, subject to the disclosure requirements in Section 9.5.
- (b) **Quantitative courses.** In quantitative courses (including Accounting, Economics, and Statistics), AI use for data analysis and modelling is permitted, subject to verification and disclosure.
- (c) **Qualitative research.** In qualitative research, AI use for transcription, coding, and thematic analysis is permitted, subject to the researcher's responsibility for interpretation and analysis.
- (d) **Creative and journalistic work.** In creative and journalistic work, AI use shall be disclosed where it materially contributes to the submitted work, and students shall not present AI-generated content as their own original creative work.

39.7 Postgraduate Studies

The College of Postgraduate Studies encompasses PGD, M.Sc., MPhil, and Ph.D. programmes across multiple disciplines. The following special provisions apply:

- (a) **Thesis and dissertation AI use.** Postgraduate students may use AI tools in their thesis and dissertation work in accordance with the categories and disclosure requirements established in this policy, as detailed in Section 14.1.
- (b) **Supervisor oversight.** Supervisors shall provide guidance, maintain oversight, and verify AI use in their students' research, as detailed in Section 14.2.
- (c) **Examination considerations.** Examiners shall be provided with guidance on AI-related issues, and viva voce examinations shall provide an opportunity to probe the candidate's understanding of their AI use, as detailed in Section 14.3.
- (d) **Research integrity training.** All postgraduate students shall receive research integrity training that includes AI-related content before commencing substantive research work, as detailed in Section 14.4.

39.8 JUPEB Foundation School

The JUPEB Foundation School prepares students for direct entry into university programmes. The following special provisions apply:

- (a) **Foundational AI literacy.** JUPEB students shall receive foundational AI literacy instruction appropriate to their level, including basic concepts, ethical use, and academic integrity requirements.
- (b) **Simplified disclosure.** AI use disclosure requirements for JUPEB students shall be simplified and age-appropriate, while maintaining the principles of honesty and transparency.
- (c) **Preparation for university.** JUPEB students shall be prepared for the more detailed AI governance requirements they will encounter at the degree level.

Section 40: Transitional Arrangements

40.1 Effective Date of the Policy

This policy shall take effect on the date approved by the Senate, or such other date as the Senate may specify. The effective date shall be communicated to the University community through the channels described in Section 36.

40.2 Grace Period for Compliance

Recognising that the implementation of this policy requires changes to teaching practices, administrative processes, and student habits, the University shall establish a grace period for compliance. The grace period shall:

- (a) **Extend for one academic semester** from the effective date for course-level AI use statements, assessment redesign, and administrative AI tool registration;
- (b) **Extend for one academic year** from the effective date for the full implementation of AI literacy requirements in existing courses;
- (c) **Not apply to prohibitions** on malicious AI use, academic misconduct, or data protection violations, which shall be enforced from the effective date;
- (d) **Be subject to review** by the AI Policy Committee, which may recommend extension or adjustment to the Senate.

During the grace period, the University shall prioritise support, guidance, and education over enforcement.

40.3 Grandfathering of Existing AI Tools and Practices

AI tools and practices already in use at the University at the effective date of this policy shall be grandfathered as follows:

- (a) **Existing AI tools.** Tools already in use shall be permitted to continue in use for a period of six months, within which time they shall be submitted for approval in accordance with Section 25.2;
- (b) **Existing research projects.** Research projects already approved and underway shall comply with this policy's disclosure requirements but shall not be required to undergo retrospective ethical review;
- (c) **Existing course designs.** Courses already designed and approved may continue as designed for one academic session, after which AI use statements shall be added in accordance with Section 9.3;
- (d) **Existing administrative practices.** Administrative practices involving AI shall be reviewed within six months and brought into compliance with this policy.

40.4 Interim Governance Arrangements

Pending the full establishment of the governance structures described in Section 29, the following interim arrangements shall apply:

- (a) **Interim AI Policy Committee.** The Vice-Chancellor shall appoint an interim AI Policy Committee within thirty days of the effective date, which shall serve until the full Committee is constituted by the Senate;
- (b) **Interim guidance.** The interim Committee shall issue interim guidance to staff and students on AI use, drawing on the provisions of this policy and any existing University policies;
- (c) **Interim contact point.** The ICT Directorate shall serve as the interim contact point for AI-related queries and concerns;
- (d) **Interim reporting.** The interim Committee shall report to the Vice-Chancellor, who shall report to the Senate as required.

40.5 First Review Timeline

The first comprehensive review of this policy shall be conducted within eighteen months of the effective date, or such earlier date as the Senate may determine. The review shall assess:

- (a) The effectiveness of the policy in achieving its objectives;
- (b) The adequacy of the grace period and transitional arrangements;
- (c) Compliance levels and any enforcement challenges;
- (d) Emerging AI developments and their implications;
- (e) Recommendations for amendment or continuation of the policy.

The AI Policy Committee shall prepare a review report for the Senate, including recommendations for amendments or continuation of the policy.

Section 41: Interpretation and Definitions (Consolidated)

41.1 Full Glossary of Terms

This Section consolidates the definitions provided in Section 4 and adds additional terms used throughout this policy.

Academic Integrity: The commitment to honesty, fairness, and responsibility in academic work, including the avoidance of cheating, fabrication, plagiarism, and other forms of academic dishonesty.

AI Policy Committee: The committee established under Section 29.3 to oversee the implementation of this policy.

AI System: Any system that uses artificial intelligence, including machine learning, natural language processing, computer vision, or generative AI.

AI Use Disclosure Form: The form provided in Appendix B for students to disclose their AI use in assessments.

Algorithmic Bias: Systematic and unfair discrimination in AI outputs arising from biased training data, flawed model design, or biased deployment contexts.

Artificial Intelligence (AI): The simulation of human intelligence processes by computer systems, including systems that perform tasks requiring human-like cognition such as learning, reasoning, problem-solving, perception, language understanding, and decision-making.

Automated Decision-Making: The process of making decisions about individuals using AI or algorithmic systems without meaningful human involvement.

College AI Representative: The representative designated by each College under Section 29.4 to serve as the primary liaison between the College and the AI Policy Committee.

Data Controller: A person or organisation that determines the purposes and means of processing personal data, as defined under the NDPA.

Data Protection Impact Assessment (DPIA): A systematic assessment of the risks to data subjects' rights and freedoms arising from processing operations, required under the NDPA for high-risk processing.

Data Protection Officer (DPO): The officer designated by the University under Section 19.4 to ensure compliance with the NDPA and this policy.

Data Subject: An individual whose personal data is processed.

Generative AI: AI systems capable of generating new content in response to prompts or inputs.

Human Oversight: The meaningful involvement of a human being in reviewing, approving, or overriding AI-generated recommendations, decisions, or outputs.

Large Language Model (LLM): A type of generative AI system trained on vast quantities of text data to understand and generate human-like language.

Machine Learning: A subset of AI in which systems learn patterns from data and improve their performance on specific tasks without being explicitly programmed.

Nigeria Data Protection Act 2023 (NDPA): The principal legislation governing the processing of personal data in Nigeria.

Nigeria Data Protection Commission (NDPC): The regulatory body established under the NDPA.

Nigerian Ethical AI Framework (NEAIF): An independently developed ethical governance framework for AI in Nigeria.

Personal Data: Any information relating to an identified or identifiable natural person.

Prompt: The input, instruction, or query provided by a human user to an AI system.

Reflective AI Use Statement: A written reflection on the role of AI in the student's learning process and the strengths and limitations of the AI tools used.

Research Ethics Committee (REC): The University committee responsible for the ethical review of research involving human participants, personal data, or potential harm.

Sensitive Personal Data: Personal data revealing racial or ethnic origin, political opinions, religious beliefs, health status, sexual orientation, or biometric data, as defined under the NDPA.

Training Data: The data used to develop, train, or fine-tune an AI model.

University: McPherson University.

41.2 Rules of Interpretation

The rules of interpretation set out in Section 4.16 shall apply to this policy.

41.3 Severability

If any provision of this policy is held to be invalid, illegal, or unenforceable, the remaining provisions shall continue in full force and effect. The invalid provision shall be replaced by a valid provision that most closely reflects the original intent.

41.4 Waiver

No waiver of any provision of this policy shall be effective unless in writing and approved by the Senate or its authorised delegate. A waiver of any breach shall not constitute a waiver of any subsequent breach.

Section 42: Appendices

Appendix A: AI Use Categories (Five-Level Scale)

This Appendix provides detailed descriptors for each of the five AI use categories established in Section 9.2.

Category 1 — No AI Permitted

Element	Description
Permitted use	None. AI tools of any kind are prohibited for the completion of the assessment.
Rationale	To assess the student's unaided knowledge, skills, or reasoning.
Typical assessments	Closed-book examinations, invigilated assessments, foundational knowledge tests.
Disclosure	Not applicable. Any AI use constitutes misconduct.

Category 2 — AI for Preparation Only

Element	Description
Permitted use	AI may be used for study, revision, and preparation, but not for the generation of the submitted work.
Rationale	To allow AI-assisted learning while requiring independent demonstration of knowledge and skills.
Typical assessments	Essays, problem sets, traditional examinations where preparation outside the assessment is permitted.

Element	Description
Disclosure	Not required, provided AI output does not appear in the submitted work.

Category 3 — AI as Language and Structure Support

Element	Description
Permitted use	AI may be used for grammar, spelling, punctuation, translation, and stylistic suggestions. Substantive content must be the student's own.
Rationale	To support clarity and correctness of expression without substituting for intellectual work.
Typical assessments	Essays, reports, presentations where language quality is not the primary assessment criterion.
Disclosure	Brief disclosure required (e.g., in assessment cover sheet).

Category 4 — AI as Research and Analysis Assistant

Element	Description
Permitted use	AI may be used for research assistance, data analysis, coding support, or generation of draft materials that the student substantially rewrites and develops.
Rationale	To develop competence in working with AI as a research and analytical tool.
Typical assessments	Research projects, data analysis assignments, coding tasks.

Element	Description
Disclosure	Detailed disclosure required (Appendix B), plus Reflective AI Use Statement (Appendix C) for major projects.

Category 5 — AI-Integrated Work

Element	Description
Permitted use	AI is a permitted and expected component of the work, with documented use and critical evaluation of AI outputs as part of the assessment.
Rationale	To develop advanced AI literacy and the ability to work effectively and critically with AI systems.
Typical assessments	AI-focused projects, assessments where AI collaboration is an explicit learning outcome.
Disclosure	Detailed disclosure required (Appendix B), plus Reflective AI Use Statement (Appendix C) and critical evaluation of AI outputs.

Appendix B: AI Use Disclosure Form

McPherson University — AI Use Disclosure Form

Instructions: Complete this form for any assessment where AI use is permitted under Categories 3, 4, or 5, or where disclosure is otherwise required. Submit this form with your assessment.

Section	Details
Student Name	
Student ID	
Course Code and Title	
Assessment Title	
Date of Submission	

AI Tool(s) Used

Tool Name and Version	Purpose of Use

Description of AI Use

Describe how AI was used in the preparation of this assessment. Be specific about which components of the work involved AI and which components were independently produced.

Prompts or Instructions Given

Summarise the key prompts or instructions you gave to the AI tool(s).

Incorporation of AI Output

Explain how the AI output was incorporated into your submitted work, including any modifications, verification, or critical evaluation you performed.

Declaration

I declare that:

- (a) The information provided in this form is accurate and complete.
- (b) I have reviewed and take responsibility for the accuracy and integrity of the final submission.
- (c) I understand that failure to disclose AI use as required, or providing false or misleading disclosure, constitutes academic misconduct.

Student Signature	
Date	

Appendix C: Reflective AI Use Statement Template

McPherson University — Reflective AI Use Statement

Instructions: Complete this statement for assessments in Categories 4 and 5, or where otherwise required. The statement should be approximately 200–300 words.

Section	Details
Student Name	
Student ID	
Course Code and Title	
Assessment Title	

Reflection Questions

Please address the following questions in your statement:

1. **Purpose.** Why did you choose to use AI for this assessment? What did you hope to achieve?
2. **Process.** How did you use the AI tool(s)? Describe your process, including how you formulated prompts, evaluated outputs, and integrated AI-generated content with your own work.
3. **Critical Evaluation.** What were the strengths and limitations of the AI tool(s) you used? Were there any inaccuracies, biases, or limitations in the AI outputs? How did you address these?
4. **Learning.** What did you learn from using AI for this assessment? How has this experience affected your understanding of AI's role in your discipline?
5. **Integrity.** How did you ensure that your use of AI was consistent with the University's academic integrity standards?

Reflective Statement

Student Signature	
Date	

Appendix D: Privacy and Responsible Use Checklist

McPherson University — AI Privacy and Responsible Use Checklist

Purpose: This checklist is provided to assist staff and students in using AI tools responsibly and in compliance with data protection requirements. It should be used before using any AI tool that processes personal data.

Before Using an AI Tool

- ☐ **Check approval status.** Is the AI tool on the University's approved list? If not, has authorisation been obtained?
- ☐ **Review the privacy policy.** Have you read the AI tool's privacy policy and terms of service?
- ☐ **Check data usage terms.** Does the tool claim rights to use your data for training or other purposes?
- ☐ **Assess data sensitivity.** What categories of data will you input? Is it personal data? Sensitive personal data? Confidential University data?
- ☐ **Verify lawful basis.** Do you have a lawful basis for processing personal data with this tool (consent, contract, legal obligation, etc.)?

When Using an AI Tool

- ☐ **Minimise data.** Input only the minimum data necessary for the task.
- ☐ **Avoid sensitive data.** Do not input sensitive personal data unless explicitly authorised and appropriate safeguards are in place.
- ☐ **Avoid confidential data.** Do not input confidential University data, examination papers, or research data not yet published.
- ☐ **Use new conversations.** Start a new conversation for each task to prevent cross-contamination of data.
- ☐ **Check outputs.** Verify AI outputs for accuracy, bias, and appropriateness before use.

After Using an AI Tool

- ☐ **Delete history.** Delete conversation history if the tool allows it and if the data is no longer needed.
- ☐ **Document use.** Record your AI use in accordance with this policy's disclosure requirements.
- ☐ **Report concerns.** Report any privacy, security, or ethical concerns to the AI Policy Committee or the DPO.

Remember: You are responsible for the accuracy and integrity of any work that incorporates AI outputs. AI is a tool, not a substitute for your own judgment and responsibility.

Appendix E: AI Tool Evaluation Criteria

McPherson University — AI Tool Evaluation Criteria

Purpose: This Appendix provides criteria for evaluating AI tools and services for potential institutional adoption or approval.

Category	Criteria	Assessment
Data Protection	Compliance with NDPA and GAID	
	Data processing agreement availability	
	Data subject rights facilitation	
	Data localisation compliance	
Data Ownership	Clarity on data ownership	
	Restrictions on vendor use of data	
	Data portability and export	
Security	Encryption (at rest and in transit)	
	Access controls	
	Incident response procedures	
	Security certifications	
Transparency	Clarity on AI models and training data	
	Disclosure of limitations	

Category	Criteria	Assessment
Reliability	Explainability of outputs	
	Service level commitments	
	Track record and references	
	Financial stability of vendor	
Ethical Practices	Bias assessment and mitigation	
	Fairness and non-discrimination	
	Human rights considerations	
Functionality	Suitability for intended purpose	
	Usability and accessibility	
	Integration with existing systems	
Support and Training	Training resources	
	Technical support	
	Documentation	
Cost	Licensing or subscription costs	
	Implementation costs	
	Ongoing maintenance costs	

Category	Criteria	Assessment
	Cost-effectiveness	
Exit and Portability	Ease of exit	
	Data portability	
	Contractual exit provisions	

Appendix F: Data Privacy Impact Assessment Template

McPherson University — Data Privacy Impact Assessment (DPIA) Template

Instructions: Complete this template for any AI system that processes personal data and is likely to result in a high risk to the rights and freedoms of data subjects, in accordance with Section 19.5.

1. Description of Processing

Item	Details
AI System Name	
Purpose of Processing	
Categories of Personal Data	
Categories of Data Subjects	
Lawful Basis	
Recipients of Data	
International Transfers	
Retention Period	

2. Necessity and Proportionality Assessment

Question	Response
Is the processing necessary for the stated purpose?	
Are there less intrusive alternatives?	
Is the processing proportionate to the purpose?	
How will data subject rights be facilitated?	

3. Risk Assessment

Risk	Likelihood	Severity	Mitigation

4. Consultation

Consultation With	Date	Outcome
Data Protection Officer		
AI Policy Committee		
Other stakeholders		

5. Authorisation

Role	Name	Signature	Date
Data Protection Officer			
AI Policy Committee Chair			

Appendix G: AI Incident Reporting Form

McPherson University — AI Incident Reporting Form

Instructions: Use this form to report any AI-related incident, including security breaches, data breaches, ethical concerns, system failures, or policy violations.

Section	Details
Reporter Name	
Reporter Contact	
Date of Incident	
Date of Report	

Incident Details

Item	Details
AI System or Tool Involved	
Nature of Incident	
Description of Incident	
Data Involved (if any)	
Individuals Affected (if any)	
Immediate Actions Taken	

Incident Category

- ☐ Data breach involving personal data
- ☐ Security breach
- ☐ System failure or malfunction

☐ Ethical concern (bias, discrimination, etc.)

☐ Policy violation

☐ Academic misconduct

☐ Other (please specify)

Reported To

Role	Name	Date
AI Policy Committee		
Data Protection Officer		
ICT Directorate		

For Official Use Only

Item	Details
Incident Reference Number	
Investigation Status	
Outcome	

Appendix H: NUC AI Policy Framework Alignment Matrix

This Appendix demonstrates how McPherson University's AI Policy aligns with the NUC's Artificial Intelligence Policy Framework and Implementation Roadmap.

NUC Framework Element	McPherson University Policy Provision
Retain human judgment in accreditation and licensing	Section 5.1 (Human-Centred Governance); Section 16.5 (Automated Decision-Making Restrictions)
Integrate AI competencies and ethics under CCMAS	Section 10.1 (Embedding AI Literacy); Section 6.2 (CCMAS Integration)
Establish AI governance committees	Section 29.3 (AI Policy Committee)
Annual Senate policy review	Section 32.2 (Scheduled Policy Review)
Periodic NUC compliance monitoring	Section 31.6 (NUC Compliance Monitoring Preparation)
Enhanced human capacity development	Section 26 (AI Literacy and Training)
Strengthen institutional data governance	Section 19 (Data Protection Framework); Section 20 (Institutional Data Governance)
Investment in high-compute infrastructure	Section 22.4 (Computing Resources for AI)
Unified regulatory guardrails	Section 6.1 (NUC AI Policy Framework); Section 6.8 (NUC Compliance Monitoring)

Appendix I: NAIS Pillar Alignment Matrix

This Appendix demonstrates how McPherson University's AI Policy aligns with the pillars of the Nigeria National Artificial Intelligence Strategy 2025–2029.

NAIS Pillar	McPherson University Policy Provision
Building Foundational AI Infrastructure	Section 22 (ICT Infrastructure and AI Readiness)
Building a World-Class AI Ecosystem	Section 28 (Research and Innovation Promotion); Section 26 (AI Literacy and Training)
Accelerating AI Adoption Across Key Sectors	Section 10 (AI Literacy and Student Development); Section 15 (Administrative Use of AI)
Ensuring Responsible and Ethical AI	Part Two (Governing Principles); Section 13 (Research Ethics and AI); Section 19 (Data Protection)
Developing a Robust Governance Framework	Part Nine (Governance and Accountability)

Appendix J: Glossary of Technical Terms

Term	Definition
Algorithm	A set of rules or instructions followed by a computer to perform a task.
API (Application Programming Interface)	A set of protocols that allows different software applications to communicate with each other.
Chatbot	A computer program designed to simulate conversation with human users, often using AI.
Cloud Computing	The delivery of computing services (including storage, processing, and software) over the internet.
Data Mining	The process of discovering patterns in large datasets using methods at the intersection of machine learning, statistics, and database systems.
Deep Learning	A subset of machine learning using neural networks with many layers to model complex patterns.
Fine-Tuning	The process of further training a pre-trained AI model on specific data to improve its performance on a particular task.
GPU (Graphics Processing Unit)	A specialised processor originally designed for rendering images, now widely used for AI computations.
Hallucination	When an AI system generates false or misleading information that appears plausible.
Inference	The process of using a trained AI model to make predictions or generate outputs.

Term	Definition
Natural Language Processing (NLP)	A field of AI focused on the interaction between computers and human language.
Neural Network	A computing system inspired by biological neural networks, used in machine learning.
Prompt Engineering	The practice of designing and refining prompts to elicit desired responses from AI systems.
Training	The process of teaching an AI model to perform a task by exposing it to data.
Transformer	A type of neural network architecture that has become foundational for many modern AI systems, particularly in NLP.

Appendix K: Reference List

This Appendix lists the primary sources referenced in the development of this policy. References are organised by category.

Nigerian Legal and Regulatory Instruments

- Nigeria Data Protection Act 2023
- Nigeria Data Protection Act General Application and Implementation Directive 2025
- Cybercrimes (Amendment) Act 2024
- Nigeria National Artificial Intelligence Strategy 2025–2029
- National Universities Commission Artificial Intelligence Policy Framework and Implementation Roadmap
- NUC Core Curriculum and Minimum Academic Standards (CCMAS)
- National Health Research Ethics Committee Guidelines

McPherson University Policies and Documents

- Academic Integrity Policy (FAC 604)
- Information Technology Usage Policy (ADM 280)
- Institutional Review Board Guidelines (FAC Appendix 13)
- Intellectual Property Policy (ADM 245)
- Vision and Mission Statements
- Strategic Partnership Documents (BEE Solutions and Consultancy Services)

International Standards and Frameworks

- UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)
- OECD AI Principles (2019, updated 2024)
- US AI Risk Management Framework

Peer-Reviewed and Professional Sources

- Balogun Harold, "Automated Decision-Making Under the NDPA: Navigating the Line Between Automation and Regulation" (2026)
- Lexology, "Burden of Proof in Disputes Involving Automated Decision-Making in Nigeria" (2026)
- Inside Higher Ed, "Indiana University Kelley School of Business AI Communication Experience"
- Neumann University, "Four-Phase AI Implementation Framework"
- UNESCO-ICHEI, "Consensus-Driven Approach to AI Governance in Nigerian Higher Education"
- IIOE Nigeria National Centre, "National Dialogue on AI in Higher Education"

MCPHERSON UNIVERSITY

ARTIFICIAL INTELLIGENCE POLICY

McPherson University is committed to remaining at the forefront of technological innovation, academic integrity, and institutional excellence in higher education. This Artificial Intelligence Policy establishes a robust, ethical, and forward-looking governance framework designed to empower students, faculty, researchers, and administrators while safeguarding personal privacy, data sovereignty, and human dignity.

Grounded in our Christian ethical foundations and aligned fully with the National Universities Commission (NUC) AI Policy Framework, the Nigeria Data Protection Act 2023 (NDPA), and the Nigeria National AI Strategy 2025–2029, McPherson University models responsible AI leadership across the African continent.

McPherson University | Seriki-Sotayo, KM 96, Lagos-Ibadan Expressway, Ogun State, Nigeria
Official Web Portal: www.mcu.edu.ng | Policy Repository: www.mcu.edu.ng/policies/ai-policy
Inquiries: info@mcu.edu.ng | Data Protection Officer: dpo@mcu.edu.ng
© 2026 McPherson University. All Rights Reserved. Senate Approved Edition.