

Artificial Intelligence Policy

Section 1 - Purpose and Scope

(1) The University of New England (UNE) is committed to being a leader in the responsible and innovative use of Artificial Intelligence (AI). UNE sees AI as a powerful tool to enhance our teaching, learning, research, and operations.

(2) This policy provides the principles and governance to ensure UNE embraces AI's potential boldly and ethically, in service of our students and our community. It ensures that AI is adopted in a manner that is safe, reliable, transparent, equitable, and aligned with UNE's strategic aspirations and core values.

(3) This policy applies to all UNE Representatives and students engaging with AI systems in any capacity related to University teaching, learning, research, or administrative functions.

(4) This policy governs the use of artificial intelligence technologies including where these technologies are embedded within third party products. Staff are to consider this policy and its principles within the context of AI-specific vendors and products (e.g. OpenAI and ChatGPT) as well as embedded AI use within more general products suites (e.g. Copilot within Microsoft Office).

(5) Within this policy:

Part A - states the principles of this policy;

Part B - outlines governance and key responsibilities for AI use;

Part C - addresses risk management and the classification of AI systems; and

Part D - provides guidance for the use of AI in specific University activities.

Part A - Policy Principles

(6) The use of AI at UNE is governed by the principles that apply to all AI implementations. These principles are described in the University's AI Framework and Principles document. This Policy specifically related to the first four principles:

- a. Safe: AI implementations will safeguard information and ensure the physical and psychological safety of all participants. Due regard will be given to privacy, security, compliance, and environmental impact.
- b. Reliable: AI implementations will meet appropriate standards for system performance and dependability, consistent with their intended purpose and overall risk profile.
- c. Transparent: The use of AI will be clearly disclosed where appropriate. The University will maintain clear lines of accountability for AI systems, and processes will be available for individuals to challenge or seek human review of significant AI-driven decisions.
- d. Equitable: AI implementations will demonstrate a commitment to inclusion, access, and non discrimination, ensuring they enlarge opportunity for all members of the UNE community.

(7) UNE is committed to leading in ethical AI development by ensuring that Indigenous-led principles guide AI

technology deployments. Developed in partnership with Aboriginal and Torres Strait Islander peoples and knowledgeable experts, UNE will establish clear protocols for ethical engagement, professional development, and requirements for genuine partnerships. AI-related proposals and applications will work to ensure UNE's AI practices uphold Indigenous rights, self-determination, and epistemic sovereignty.

Part B - Governance and key responsibilities for AI

(8) The University will maintain clear lines of accountability for the oversight of AI systems.

(9) Specific responsibilities for the governance and oversight of AI are outlined in the below table:

Role	Responsibility
University Council	Approves the AI Policy and provides oversight of AI-related strategic risks.
Vice-Chancellor and Chief Executive Officer	Champions the responsible use of AI and ensures University-wide compliance with this policy.
Executive Team	Provides strategic direction and ensures the resourcing of AI initiatives in alignment with University goals. The Executive is kept informed of AI deployments across the University and is notified of technology procurement that introduces new AI toolsets into the University's technology landscape.
Academic Board and Committees	Provides oversight of academic matters in relation to curriculum design, assessment design, student experience and other matters within the scope of Board and each of its Committees.
AI Sponsor	Initiates and is accountable for the outcomes and risks of an AI system within their area of responsibility.
AI Operator	Day-to-day management, monitoring, and maintenance of an approved AI system.
AI User	Uses AI systems ethically, for their intended purpose, and in accordance with this policy and associated guidelines.

Part C - Risk Management and Classification of AI Systems

(10) The University encourages innovation and experimentation with new technologies within a framework of appropriate risk-based safeguards.

(11) AI systems will be classified according to the following risk framework to ensure oversight is proportionate to the potential impact:

Core Risk Dimension	Low Risk Scenario (1)	Medium Risk Scenario (2)	High Risk Threshold (3)
System Security	Internal/Isolated: secure system, source data is not used to train the model.	Internal/Shared: data processing involves public-facing components, moderate risk of data exposure.	Public/Personal Sensitive: high potential for data leakage, system is public-facing and processes sensitive data, security failure jeopardises core operations.
Data Sensitivity	Public: only processes general, non-sensitive or publicly available information (eg. news articles, meeting minutes).	Institutional: processes anonymised institutional data or basic personal contact information.	Personal/Sensitive: processes sensitive personal information (eg. health status, protected characteristics), financial data, data requiring specific regulatory protection.

Core Risk Dimension	Low Risk Scenario (1)	Medium Risk Scenario (2)	High Risk Threshold (3)
Usage & Autonomy	Informational: supporting decision making (eg. summarise information for human review).	Decision Support: providing analysis/recommendations (eg. used to analyse a document and/or data and provide recommendations).	Automated Decision: autonomous decision making (eg. AI makes a final determination on a matter or provides direct advice to a student).
Transparency	Fully transparent: AI use is fully visible, documented and explicitly consented to by the user/affected party.	Partially transparent: AI is used in the background for efficiency, but its involvement is not immediately obvious to the user.	Opaque/Covert: lack of clear disclosure that AI is being used in a decision making process, covert or manipulative function.

(12) The AI Systems Use Framework (outlined below) classifies use according to the aggregated risk scores generated from the above AI Risk Framework (5 and below indicating the lowest level of risk and 6-10 indicating Medium Risk and 11-15 indicating the highest level of risk). It also outlines the associated record keeping, reporting and monitoring requirements in alignment with associated risk scores, and prohibited AI use.

Aggregated Risk	Definition and Application	Required Record Keeping and Reporting	Required Monitoring/Oversight Level
Low Aggregate Risk Score (5 and below): Permitted	Low-risk applications where the AI's function is transparent, uses non-sensitive data, and acts primarily for brainstorming, summarisation, or low-autonomy decision support.	Registration maintained at the Local Business Area; periodic summary reporting to Management.	By Exception (Monitoring is only triggered if a policy breach, incident, or unexpected outcome is reported.)
Medium Aggregate Risk Score (6-10): Localised risk assessment required	Applications with a medium aggregate risk profile, typically contained within a local business unit, where assessment confirms the risk can be effectively managed locally.	Risk assessment by local manager; record in inventory (Local Business Area).	Periodic review(Scheduled audits and checks).
High Aggregate Risk Score (11-15 and below): AI Governance Approved	High-risk applications involving sensitive data, high potential impact on an individual's rights or access to services, or highly autonomous function.	Detailed risk assessment and approval documented; ongoing usage statistics reported to Management (small 'g' governance).	Periodic (Scheduled audits and reviews focused on performance, bias detection, and compliance) or Ongoing (for high-volume or high-impact systems).
Prohibited	Use cases that pose unacceptable risks, contravene University values, or violate legal/policy thresholds (e.g., systems for covert surveillance, social scoring, or autonomous high-impact decisions).	Policy and compliance status reported to Council; detailed accountability reporting on boundary enforcement.	Ongoing (Active institutional monitoring and auditing to ensure non-deployment and boundary compliance.)

(13) All AI systems classified as Medium Risk or High-Risk Threshold risk must include a risk assessment that is recorded as per the University's [Records Management Rule](#), and High-Risk use must be approved by the Executive Team following a formal risk assessment prior to implementation.

Part D - Use of AI in specific University activities

(14) The following clauses provide specific guidance for the application of AI in key University activities.

Teaching, Learning, and Assessment

(15) The use of AI in academic activities must uphold academic integrity. Where used to support teaching or assessment, its application must be transparent, equitable, and enhance the student learning experience. All uses of AI in formal assessment must be managed in strict adherence to the [Student Academic Integrity Policy](#), [Assessment Policy](#), and [Assessment Appeals Policy](#).

(16) Staff use of AI tools must rigorously comply with the [Knowledge Assets and Intellectual Property Policy](#), [Copyright Policy](#), [Information and Communication Technology Facilities and Services Rule](#), [Information Security Rule](#), and [Privacy Management Rule](#). Staff must not input confidential, commercial-in-confidence, or personal information (including staff, student, or financial data protected under the Australian Privacy Principles) into AI systems unless the system's security, data usage terms, and compliance with the UNE [Privacy Management Rule](#) are formally verified and approved.

(17) In alignment with the [Freedom of Speech Rule and Academic Freedom Statement](#), the [Freedom of Speech and Academic Freedom Policy](#) and the [UNE Academic and English Language Teaching Staff Enterprise Agreement 2024-2026](#), individual academic staff members retain the right to opt out of using specific institutionally recommended AI tools or methodologies within their independent design of curricula, methods of teaching, or research activity, provided that opting out does not compromise mandatory compliance, core unit learning outcomes, or established professional standards.

Research

(18) Researchers and HDR Candidates using AI must adhere to the [Australian Code for the Responsible Conduct of Research](#), [Code of Conduct for Research Rule](#), and transparently report its use in all methodologies and publications.

(19) All Higher Degree Research (HDR) Candidates utilising Artificial Intelligence tools in their research activities, including for data analysis, synthesis, or drafting, must do so in strict accordance with the provisions outlined in the [HDR - Avoiding Plagiarism and Academic Misconduct \(Higher Degree Research\) Guideline](#).

Professional and Operational Activities

(20) The use of AI to support University operations should aim to improve efficiency and effectiveness.

(21) To ensure the protection of University information, all professional and operational activities must comply with the following:

- a. University-Approved Enterprise AI Systems: Systems that have been formally approved and have enterprise-level security and data protection (eg UNE's Madgwick platform), may be used to enter University information, including personal or confidential data, in accordance with the system's specific terms of use and the [Knowledge Assets and Intellectual Property Policy](#), [Copyright Policy](#), [Information and Communication Technology Facilities and Services Rule](#), [Information Security Rule](#), and [Privacy Management Rule](#).
- b. Public or External AI Systems: Publicly available AI tools not formally contracted by the University (eg, free versions of ChatGPT, Gemini, etc.). Personal, confidential, or commercially sensitive University information must not be entered into these systems. Only public, non-sensitive data may be used.

(22) All complaints, grievances, or reported breaches concerning the use of AI, including matters related to academic integrity, privacy, or intellectual property, must be lodged following the formal requirements of the [Student Academic Integrity Policy](#), [Information and Communication Technology Facilities and Services Rule](#), [Information Security Rule](#), [Privacy Management Rule](#), [Staff Misconduct Policy](#), [Student Conduct Rule](#) and [Data Breach Policy](#). A dedicated triage process will determine the appropriate governance pathway. Issues requiring policy interpretation, system safety review, or potential amendment to the AI Governance Framework or this Policy will be formally escalated to the AI Governance Committee for academic review and necessary resolution.

Section 2 - Authority and Compliance

Authority

(23) The University Council, pursuant to Section 29 of the [University of New England Act 1993](#) makes this University Policy.

(24) All UNE Representatives and students must observe this Policy in relation to University matters. The Office of the Executive Director Future Students, Engagement and Technology can provide guidance on matters covered by this Policy.

(25) The Executive Director Future Students, Engagement and Technology is authorised to make procedures and processes for the effective implementation and operation of this policy, and to publish as associated documents any tool that will assist with compliance.

Compliance

(26) This policy is consistent with the [Higher Education Standards Framework \(Threshold Standards\) 2021](#), the NSW Government AI Assurance Framework, the principles of the [Australian Artificial Intelligence Ethics Framework \(AAIEF\)](#). The policy will be regularly reviewed to ensure consistency with other statutory obligations in relation to the use of AI.

(27) This policy operates as and from the Effective Date. Previous policy on the use of AI are replaced and have no further operation from the Effective Date.

(28) Notwithstanding the other provisions of this policy, the Vice-Chancellor and Chief Executive Officer (VC&CEO) may approve an exception to this Policy where the VC&CEO determines the application of this Policy would otherwise lead to an unfair, unreasonable or absurd outcome. Approvals by the VC&CEO under this clause must be documented in writing and registered in the approved UNE electronic Records Management System (RMS).

Section 3 - Quality Assurance

(29) The Policy Owner will regularly monitor the operation of this policy and provide an annual attestation to the Audit and Risk Committee on compliance with the Policy, and report breaches of the Policy in accordance with the [Compliance Rule](#) and [Compliance Procedures](#).

Quality Assurance Measures

QA Measures	QA Body and Reporting
Annual review of the AI Policy to ensure it remains current with technological advancements and regulatory changes.	EDFSET reports review outcomes to the Executive Team.
Regular audit of the AU Systems Inventory to ensure high-risk systems are registered and have completed risk assessments.	Internal Audit reports to the Audit and Risk Committee.
Monitoring and reporting breaches of this policy.	Governance Directorate reports to the Policy Owner and relevant committees as per the Compliance Rule .
Assurance of strategic AI risk oversight.	The Audit and Risk Committee provides assurance on strategic risks to the University Council.
Review of AI literacy and training programs to ensure they remain effective and relevant for staff and students.	EDFSET reports to the Executive Team and Academic Board.

Section 4 - Definitions

(30) Artificial Intelligence (AI) – Technologies that are designed to perform tasks that would typically require human intelligence, such as learning, reasoning, problem-solving, and understanding language.

(31) AI System - An IT system that incorporates one or more AI technologies.

(32) AI Sponsor - A senior leader, typically a Head of a Business Unit, who initiates an AI system and is ultimately accountable for its implementation, outcomes, and risk management in alignment with this policy.

(33) AI Operator - An individual or team responsible for the day-to-day operational management of an approved AI system. This includes monitoring system performance, ensuring ongoing compliance, and acting as the first point of contact for operational issues.

(34) AI User - Any UNE Representative or student who interacts with or uses an AI system for University-related activities. The AI User is responsible for using the system ethically and in accordance with this policy.

Status and Details

Status	Current
Effective Date	2nd February 2026
Review Date	2nd February 2027
Approval Authority	Vice-Chancellor and Chief Executive Officer
Approval Date	29th January 2026
Expiry Date	Not applicable
Unit Head	Neil Durrant Executive Director Future Students, Engagement and Technology
Enquiries Contact	Neil Durrant Executive Director Future Students, Engagement and Technology <hr/> Future Students, Engagement and Technologies