AI Governance and Responsible Use Policy

Section 1 - Summary

(1) This Policy defines the governance and responsible use of Artificial Intelligence (AI) at Victoria University (VU or the University), ensuring data integrity, privacy and security, communicating obligations when using AI technologies and protecting stakeholders from the unintended consequences of AI implementations and use.

Section 2 - Scope

(2) This Policy applies to:

a. VU staff, students, visitors, contractors and third-party service providers both onshore and offshore or when connecting to IT computing facilities, systems, networks and accounts, either on University premises or remotely.
b. VU staff, students, visitors, contractors, and third-party providers engaging with AI tools—whether University-provided or publicly available.
c. The use of technologies classified as AI for VU related purposes including but not limited to Generative Artificial Intelligence (GAI), Generative Adversarial Network (GAN), Machine Learning (ML), Large Language Models (LLM), Generative Pretrained Transformer (GPT) and other subsets of Artificial Intelligence (AI).
d. Integration of AI technologies within the University's enterprise suite.
e. This Policy applies to AI technologies and processes used in support of research activities but does not govern the research itself or its outcomes. See Research Integrity Policy.
f. There are no general exclusions to this policy. However, exceptions may be made on a case-by-case basis where regulatory or specific contractual obligations require deviations, subject to approval by the designated governance authority within the University.
g. This Policy should be read in conjunction with the following policies:
    i. Academic Integrity Policy
    ii. IT Appropriate Use Policy
    iii. Appropriate Workplace Behaviour Policy
    iv. Assessment for Learning Policy
    v. Contracts Policy
    vi. IT Asset Policy
    vii. Information Security Policy
    viii. Information Security - IT Security Audit Authorities Procedure
    ix. Privacy Policy

Section 3 - Policy Statement

(3) This Policy provides a clear framework and principles to ensure the responsible and ethical use of AI technologies, its governance and application and to:

a. provide guidance on the acquisition and deployment of AI technologies.
b. govern the responsible development, use and management of AI to mitigate risks, including ethical concerns, operational vulnerabilities and risks to the University's academic and research integrity, intellectual property and data privacy.
c. ensure AI technologies comply with legal, regulatory and ethical obligations and standards, including privacy, data protection and human rights.
d. foster innovation while maintaining accountability, transparency and fairness when using AI technologies.
e. promote a culture of responsibility among user cohorts to align the use of AI tools with the University's core values and strategic goals, while minimising the potential risks and unintended consequences of AI technologies' implementation and
f. set guidelines for the responsible adoption and ethical use of AI technologies in teaching, learning and research and business.

Part A - AI Governance Principles

(4) VU's core AI Governance Principles have been developed to guide the responsible use, development and management of AI technologies across the University in alignment with the Australia's AI Ethics Principles.

Core AI Governance Principles

a. Empowerment and Positive Impact: Enable ethical, productive use of AI that enhances learning, teaching, research and operational efficiency.
b. Fairness and Equity: Ensure AI technologies are accessible to all and used in ways that are free from bias and discrimination, supporting inclusive outcomes.
c. Transparency and Accountability: Clearly communicate how AI tools work, who is responsible, and how decisions are made—fostering trust through openness.
d. Privacy and Security: Protect personal data and prioritise robust cybersecurity practices across all AI-enabled systems.
e. Academic and Ethical Integrity: Preserve the integrity of academic work, research standards, and institutional values through ethical AI practices.
f. Wellbeing and Social Benefit: Design and use AI for the benefit of individuals, communities, and the environment—avoiding harm and enhancing human outcomes.
g. Upskilling and Literacy: Support students and staff to develop the skills needed to use AI ethically, confidently, and critically in a world where AI is pervasive.
h. Ongoing Evaluation and Risk Mitigation: Continuously assess AI tools for reliability, relevance, and risk—adapting guardrails as technologies and contexts evolve.

Part B - AI Governance Framework

AI Steering Committee

(5) The AI Steering Committee will be established as the authoritative management committee overseeing the strategic enablement, responsible use, and enterprise coordination of AI at Victoria University. It will report through the Vice-Chancellor's Group (VCG) and will be added to the VCG workplan to ensure executive visibility and alignment.

(6) The AI Steering Committee will work closely with the Data Governance Committee to:

a. Review and update data governance policies to address AI-specific needs.
b. Establish data quality standards for AI applications.
c. Develop guidelines for the responsible handling of data used to train AI systems.
d. Implement appropriate data retention policies for AI systems.

The membership of the AI Steering Committee will be outlined in the related Procedure document. It will include representation from across the university, including academic and research domains, to ensure balanced input into decision-making and prioritisation.

AI Risk Classification

(7) The AI Risk Classification Model is used to classify AI technologies based on their potential impact, data sensitivity, level of automation, and associated legal, ethical, and reputational risks.

Provisions for Human oversight and Contestability of AI decisions

(8) All AI systems must have appropriate human oversight, proportionate to the Risk Level (see AI Risk Classification Model) assigned to the AI system.

(9) All AI systems that support, influence or make decision affecting individuals must:

a. provide ways for humans to review and intervene in those decisions.
b. have an assigned responsible and accountable owner.
c. ensure human judgment is the final authority for important decisions; and
d. establish provisions that allow individuals to contest AI-driven decisions where appropriate.
e. Students and staff may utilise the University's standard complaint or grievance channels for any disputes related to AI. See Staff Complaints Resolution Policy and Student Complaints Policy.

Part C - Use of AI Technologies

(10) VU promotes a flexible, principles-based (See Part A – AI Governance Principles) approach to the responsible use of AI technologies across academic, research and business contexts that enables innovation while safeguarding individuals, communities and VU values.

(11) VU provides a suite of AI tools that are University-licensed, supported, and assessed for alignment with VU policies and standards. These AI tools are recommended for use where possible, and can be used in teaching, research, and administration activities without prior approval on condition users comply with this Policy.

(12) Users that choose to explore alternative AI tools (including open-source and publicly available platforms) for individual use are requested to assess these tools using the AI Risk Classification Model and follow relevant guidelines provided by the AI committee.

(13) Users of alternative AI tools must ensure they comply with the principles (See Part A – AI Governance Principles) of responsible use, applicable legislation, and University policies and procedures including the AI Governance and Responsible Use Procedure (to be established).

(14) VU does not seek to regulate all AI technologies exhaustively, however, may prohibit certain AI tools for university use based on strategic alignment, legislation, and regulations, risk assessment, and ethical evaluation to protect the integrity, privacy, transparency, and security of VU data.

Responsible Use

(15) Users are required to use AI technologies in an appropriate, responsible and ethical manner and in line with this Policy.

(16) Users are expected to safely engage with AI technologies when using AI to enhance productivity, decision-making and service delivery to the benefit of staff and students.

(17) Users must be aware that generative AI can produce realistic content that may be difficult to distinguish from human-created work and may contain inaccuracies or 'hallucinations.' Such content, while appearing credible, can unintentionally mislead, influence important decisions or contribute to the spread of misinformation if accepted without critical evaluation.

(18) Users are encouraged to explicitly disclose when content has been generated using AI to support transparency and mitigate the risk of misinformation.

(19) Users must ensure they critically evaluate AI-generated content for accuracy, impartiality, and limitations and are responsible for verifying the information to ensure the reliability of the content before use.

(20) The use of AI in research activities must comply with data security frameworks, this Policy and the Research Integrity Policy, Research Integrity - Authorship Procedure, Research Integrity - Research Data Management Procedure.

(21) VU reserves the right to deploy AI system monitoring and web filtering capabilities in line with Information Security Policy to ensure the use of AI technologies is lawful and complies with university values and policies.

(22) VU will provide users educational training and awareness programs to support users to engage with AI technologies ethically, responsibly and effectively.

(23) Only authorised users with a legitimate business purpose may access training data used for AI technologies or AI outputs involving sensitive or identifiable data.

Unacceptable Use

(24) The following is inappropriate and prohibited when accessing or using AI technologies:

a. Engaging in any activity that is illegal or unlawful under State, Federal or International law or in breach of any University policy including the IT Appropriate Use Policy and Appropriate Workplace Behaviour Policy.
b. Use that violates the Copyright Policy and Intellectual Property Regulations 2013.
c. Misrepresenting AI-generated work as original student work in breach of the Academic Integrity Policy.
d. Use of any AI technologies or platforms that are classified as 'Unacceptable' under the University's AI Risk Classification Model or are banned by government authorities. This includes tools that pose significant risks to data privacy, academic integrity, security, or compliance with legal and regulatory obligations.

Learning and Teaching

(25) Staff may use AI technologies to support the assessment of or feedback on students' work, provided they comply with this Policy and the Assessment for Learning Policy and retain responsibility for making evaluative judgements regarding students submitted work or any feedback given.

(26) Student use of AI technologies must comply with this Policy and the Academic Integrity Policy and Academic Integrity Guidelines.

(27) Specific rules on student use of AI technologies may be set by the subject educator. Depending on the course, unit, or discipline, and the intended learning outcomes, AI tool usage may be restricted, prohibited, or actively encouraged. Users must comply with these guidelines as outlined by their course requirements.

(28) Students are generally permitted to use University-approved AI tools to enhance their personalised learning and assist in preparing assessed work, however must appropriately disclose the use of any AI-generated content in line with the Academic Integrity Policy and ensure that their contributions, whether individual or part of a group project, are original.

Intellectual Property and Copyright Considerations

(29) Under current Australian copyright law, only works created by humans can be protected. This means that output generated entirely by AI (including but not limited to content, data, code, tools, models, or recommendations) is not eligible for copyright protection. For work to be protected by copyright, it must involve a human who has made a meaningful intellectual contribution.

(30) The following principles guide the VU's position on intellectual property (IP) and copyright as they relate to AI and apply in conjunction with the Copyright Policy, Research Integrity Policy and Learning and Teaching Quality and Standards Policy:

a. Students retain ownership of their own original work and must disclose any use AI-generated content in accordance with the Academic Integrity Policy.
b. Staff remain the responsible authors of teaching materials and institutional content, including content prepared using AI tools. Such materials are considered University IP under existing arrangements.

(31) Enterprise AI tools, data pipelines or models developed by staff, contractors, or vendors within the scope of their work for the University are considered University-owned IP, unless otherwise negotiated. This includes tools built for internal automation, research, learning analytics, or administrative use.

(32) Uploading or training AI systems using University-owned data or content (including research data, student records, teaching materials or internal documents) must comply with the AI Governance and Responsible Use Procedure (to be established), Data Governance, Information Security Policy and Intellectual Property Regulations 2013.

Part D - AI System Management

(33) AI systems used for business, research and academic purposes must be selected, managed and utilised in a manner that achieves the objectives of the University and according to the principles outlined in the IT Asset - Business Application Procedure and comply with the IT Asset Policy, Purchasing Policy, Risk Management Policy, Third Party Arrangements Policy and Contracts Policy and Contracts Procedure.

(34) The procurement of AI systems, including processes for assessment, approval, and contractual arrangements with third part service providers of AI systems must include appropriate consultation and AI governance measures (see AI Risk Classification Model) prior to entering contractual commitments.

(35) All AI implementations must adhere to relevant international regulations when handling data across international borders, including when using third-party AI systems or services hosted or provided by external vendors

(36) When deploying AI systems that handle data across international borders, VU must consider:

a. Data Localisation Laws: Regulations that require data to be stored within the country where it was collected.
b. International IP Considerations: Intellectual property laws that vary between jurisdictions and affect how AI

technologies can be used and protected.

c. Privacy Variations: Differences in privacy laws and regulations between countries that impact how personal data can be processed and shared.

(37) AI systems will be subject to a full lifecycle management process proportionate to the Risk Level (see AI Risk Classification Model) assigned to the AI system.

(38) AI system lifecycle management procedures will be established and implemented in alignment with the IT Asset - Business Application Procedure, Information Security Policy and AI Governance and Responsible Use Procedure (to be established).

(39) VU maintains procedures for identifying, reporting, and responding to AI-related incidents including but not limited to system failures, data breaches and bias that align with existing incident management processes, the Information Security Policy, Critical Incident, Emergency Planning and Business Continuity Policy, Privacy Policy.

(40) VU will maintain a dedicated AI Incident Register aligned with the University's broader incident reporting systems.

(41) Academic Integrity incidents in relation to unacceptable use of AI generated content in student assessed materials are recorded in accordance with the Academic Integrity Policy.

Part E - AI Data Practices

(42) AI implementations must adhere to the University's Data Governance Framework and Data Governance Standards, with additional AI-specific data governance requirements based on the Risk Level (see AI Risk Classification Model) assigned to the AI system including:

a. Data quality assessment for AI training and operational data
b. Bias detection and mitigation in training datasets
c. Data lineage documentation for AI-processed information
d. Special handling procedures for synthetic data generated by AI.

Part F - Breach of Policy

(43) Any actual or suspected breaches of this Policy and related Procedures should be reported immediately to the relevant line manager and/or the Digital and Campus Services Desk.

(44) All breaches of this Policy will be treated seriously and may be subject to disciplinary action in accordance with the relevant enterprise agreement (for employees) or Student Misconduct Regulations 2019 (for students).

Section 4 - Procedures

(45) AI Governance and Responsible Use Procedure (to be established)

(46) AI Systems Lifecycle Procedure (to be established)

(47) AI Risk Classification Model (to be established)

Section 5 - HESF/ASQA/ESOS Alignment

(48) HESF: Standards 2.1 Facilities and Infrastructure; 3.3 Learning Resources and Support; 7.3 Information Management.

(49) Outcome Standards for NVR Registered Training Organisations 2025: Standards 1.3-1.5 Assessment; 1.8 Facilities, Equipment and Resources; 2.7, 2.8 Feedback, Complaints and Appeals; 4.3 Risk Management; 4.4 Continuous Improvement 2.1-2.2 Information.

Section 6 - Definitions

(50) Artificial intelligence (AI): The simulation of human intelligence in machines, enabling them to learn, reason, solve problems and make decisions. IT systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making and translation between languages. Is a machine-based system that infers, from the input it receives, how to generate outputs such as language processing content, recommendations or decisions.

(51) Bias in AI: Unfair advantages or disadvantages in AI outputs due to biased training data.

(52) Data Privacy: The protection of personal or sensitive information used by AI systems, ensuring compliance with laws and regulations.

(53) Ethical AI: The practice of developing and the deployment of AI systems that align with human values and moral principles, ensuring fairness, transparency, accountability, and the prevention of harm to users.

(54) Hallucination: The phenomenon where a generative AI system, such as a large language model (LLM), produces content that is incorrect, misleading, not factual, or entirely fabricated—including made-up references or citations that appear plausible but do not exist.

(55) Large Language Model (LLM): A large language model (LLM) is a specific class of machine learning model that is trained on large volumes of sample text in order to perform natural language processing tasks, such as language generation. Examples: Open AI, Chat GPT, Gemini, Llama, and xAI Grok.

(56) Users: Staff, Contractors, Consultants, third-party service providers, volunteers and Students (when working within University’s virtual and physical environments).

Section 7 - Supporting Documents and Information

(57) AI Risk Classification Model

Status and Details

Status	Not Yet Approved
Effective Date	To Be Advised
Review Date	To Be Advised
Approval Authority	
Approval Date	To Be Advised
Expiry Date	Not Applicable
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Stuart Hildyard Chief Digital Officer and Executive Director Campus Services +61 3 9919 5576
Enquiries Contact	Nea Dhillon Director, AI Technology & Delivery +61 3 9919 5894