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, controlled entities of Victoria University, 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, controlled entities of VU, and third-party providers engaging with AI tools – whether University-provided or publicly available.
c. The use of AI technologies for VU-related purposes, including tools that generate content Agentic AI, AI Coworker, (Generative AI – GAI), learn from data (Machine Learning – ML), or process language (Large Language Models – LLM, such as Generative Pretrained Transformers – GPT). Definitions of these terms are provided in the Definitions section.
d. Integration of AI technologies into the University's core operational systems, including finance, human resources, student management, and collaboration platforms.

(3) 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.

(4) 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.

(5) This Policy should be read in conjunction with the following policies:

a. Academic Integrity Policy
b. IT Appropriate Use Policy
c. Appropriate Workplace Behaviour Policy
d. Assessment for Learning Policy
e. Contracts Policy
f. IT Asset Policy
g. Information Security Policy
h. Information Security - IT Security Audit Authorities Procedure

i. Privacy Policy
j. Research Integrity Policy
k. Research Integrity - Research Data Management Procedure
l. Copyright Policy
m. Copyright Procedure

Section 3 - Policy Statement

(6) VU is committed to human-first AI enablement, using AI to create positive outcomes, drive innovation, and advance equity, while managing evolving risks through strong governance. This Policy sets out the University's approach to acquiring, developing, and using AI responsibly to uphold integrity, protect data, and foster trust through transparency and accountability. It 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;
f. set enforceable guidelines for the responsible and ethical use of AI technologies in teaching, learning, and research. This includes the requirement that any substantial contribution by AI tools to academic, research, or creative work must be transparently disclosed, to uphold academic integrity and clearly evidence genuine learning or original authorship; and,
g. ensure the accountable use of AI technologies in business operations by requiring that, where AI tools are used in ways that meaningfully influence decisions, outputs, or service delivery, their use is appropriately documented and attributable, supporting transparency and compliance with university standards and the Copyright Policy and Copyright Procedure.

Part A - AI Governance Principles

(7) Victoria University's AI principles reflect a One VU approach, aligning with our strategic goals and ethical commitment and Australia's AI Ethics Principles. These principles guide the responsible use, development, and management of AI technologies across learning, research, operations, and community engagement.

Core AI Governance Principles

(8) Ethical, Inclusive, Human-Centred AI: AI must be designed and used in ways that uphold human dignity, promote wellbeing, and support diverse identities. This includes embedding fairness, transparency, and accountability into AI systems to ensure ethical outcomes and avoid harm.

(9) Protecting Country and First Nations Perspectives: AI initiatives must respect First Nations sovereignty, knowledge systems, and cultural integrity. This includes alignment with sustainability and Country-centred design principles, and a general commitment to inclusive practices that reflect the values of all communities served by the University.

(10) Co-Intelligence: People and Technology Together: AI systems must augment human creativity, judgment, and decision-making – not replace it. Systems must support collaborative intelligence, with clear provisions for human oversight, contestability, and explainability to foster trust and accountability.

(11) Equity and Inclusion by Design: AI should act as an equaliser, closing equity gaps and supporting diverse learners, staff, and communities. This includes equitable access to AI tools and outcomes, and the use of inclusive, representative data across training and production systems to ensure AI recognises and serves all people fairly.

(12) Data as a Strategic, Ethical Asset: Data used in AI systems must be governed as a strategic resource, with robust privacy, security, and ethical standards. Transparency in data lineage, responsible use of synthetic data, and continuous evaluation are essential to maintain trust and integrity.

(13) These principles will be reviewed periodically to ensure they remain aligned with evolving technologies, societal expectations, and the University's strategic direction.

Part B - AI Governance Framework

(14) The AI Governance Framework will include clear documentation of roles and responsibilities for all parties in the AI supply chain, including internal teams and external providers. Shared accountability for monitoring, evaluation, and transparency of AI systems will be maintained throughout the lifecycle.

AI Steering Committee

(15) The AI Steering Committee is the decision-making and enterprise oversight body for AI strategy, policy, and major investments at Victoria University. It will report through the Vice-Chancellor's Group on matters to ensure executive visibility and alignment.

(16) Key responsibilities of this management committee are to:

a. Approve AI strategy, policies and major projects and decisions on usage guidelines and restrictions.
b. Monitor progress against roadmap milestones and KPIs.
c. Ensure alignment with VU's strategic plan and values.

AI Ethics and Governance Committee

(17) The AI Ethics and Governance Committee, a sub-committee of the AI Steering Committee, will have oversight of ethical, legal, and risk aspects of AI and data use. Working closely with the Data Governance Committee, it will:

a. Review and update data governance policies to address AI-specific needs.
b. Review and approve high-impact or sensitive AI projects.
c. Oversee AI-related data governance, privacy, and compliance.
d. Publish transparent reports on AI use and outcomes.

(18) The membership of the AI Steering Committee and AI Ethics and Governance Committee will include representation from across the university to ensure a One VU approach.

AI and Emerging Technologies Risk Management Working Group

(19) The AI and Emerging Technologies Risk Management Working Group Committee is an operational layer of risks associated with use of existing and onboarding new AI and emerging technologies, risk monitoring and mitigation at an enterprise level on all existing and upcoming AI and emerging technology stack, as the overarching governance is built and embedded. This working group comprises of expertise from enterprise risk, OGC, cyber security, AI

engineering, and information and privacy governance and will be accountable for maintaining oversight of and providing risk advice on new and existing AI systems. The policy expects our remit to cover (but not limited to):

a. Maintain the AI and emerging technologies Risks Register
b. Review open risks and advise on mitigation strategies
c. Maintain oversight of legal and regulatory risks associated with AI and emerging technologies adoption
d. Monitor ongoing legislative reforms and case law associated with AI and emerging technologies to ensure VU's policy framework aligns with legal obligations
e. Shaping practical governance frameworks and processes to enable effective operational oversight

(20) For any queries or questions in relation to AI risk please contact the AI and emerging Technologies Risk Management Working Group.

AI Risk Classification

(21) 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

(22) All AI systems must have appropriate human oversight, proportionate to the Risk Level (see AI Risk Classification Model) assigned to the AI system in line with the Core AI Governance Principles.

(23) AI systems influencing decisions about individuals must allow human review, accountability, and contestability, as outlined in the Core Principles.

(24) Students and staff may utilise the University's standard complaint or grievance channels for any disputes related to AI (see Complaints Policy).

Part C - Use of AI Technologies

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

(26) 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.

(27) Users who wish to use alternative AI tools (including open-source or publicly available platforms) must assess these tools using the AI Risk Classification Model and follow guidance issued by the AI Steering Committee. All AI tools in use – whether centrally provisioned or individually selected—must be registered in the AI Registry (to be established).

(28) The University reserves the right to audit AI tool usage and monitor compliance with this Policy, including verifying that tools have been appropriately assessed and registered. Access to tools may be revoked if they are found to be non-compliant.

(29) Users of any AI tools, including alternatives, are responsible for ensuring compliance with the AI Governance Principles (see Part A), applicable legislation, and relevant University policies and procedures, including the AI Governance and Responsible Use Procedure.

(30) 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

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

(32) Users must engage with AI technologies responsibly and safely to enhance productivity, support decision-making, and improve services for staff and students.

(33) 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.

(34) Users must ensure that any substantial use of AI tools in the creation of content is appropriately disclosed, to support transparency, uphold integrity, and mitigate the risk of misinformation. For guidance on what constitutes substantial use and appropriate disclosure, refer to clauses 6f and 6g of this Policy.

(35) 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.

(36) 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.

(37) 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.

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

(39) 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

(40) 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 and the ViC & AU PP.
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 and/or regulatory authorities. This includes tools that pose significant risks to data privacy, academic integrity, security, or compliance with legal and regulatory obligations.

Learning and Teaching

(41) 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.

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

(43) 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, or per the overarching guidance of the Academic Integrity Guidelines.

(44) 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

(45) 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. Consequently, VU or individuals cannot claim copyright over purely AI-generated works. For copyright protection to apply, a human must make a meaningful intellectual contribution to the work.

(46) The following principles guide 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 of 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.

(47) 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.

(48) 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, Data Governance, Information Security Policy and Intellectual Property Regulations 2013.

Part D - AI System Management

(49) 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, Contracts Policy and Contracts Procedure.

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

(51) AI risk and impact assessments must consider the broader AI supply chain, including who develops, maintains, or supplies the system, as well as who has access to the training infrastructure and data. The AI Model Intake Form will include a Supply Chain Risk Checklist and require third-party providers to disclose any AI used in service delivery, with

corresponding contract clauses to ensure transparency and oversight.

(52) 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.

(53) 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.

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

(55) 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).

(56) 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.

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

(58) 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

(59) 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

(60) 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.

(61) 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

(62) Nil.

Section 5 - HESF/ASQA/ESOS Alignment

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

(64) 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

(65) Agentic AI: AI systems designed to operate with a degree of autonomy by planning, making decisions, and taking actions to achieve defined goals within set constraints. Agentic AI may initiate tasks, interact with systems or users, and adapt its behaviour based on context, while remaining subject to human oversight and governance controls.

(66) AI Coworker: An AI–enabled system or tool that supports staff by performing tasks alongside humans, such as drafting content, analysing information, answering questions, or coordinating workflows. An AI coworker does not have legal or employment status and operates under human direction, accountability, and institutional governance.

(67) 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, image generation, speech recognition, decision-making and translation between languages. A machine-based system that infers, from the input it receives, how to generate outputs such as language processing content, recommendations or decisions.

(68) AI Supply Chain: The sequence of activities, parties, and processes involved in the development, provision, deployment, and operation of AI systems at Victoria University. This includes internal teams, external vendors, contractors, and any third-party providers who contribute to the lifecycle of an AI system.

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

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

(71) 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.

(72) Generative Artificial Intelligence (GAI): AI systems that create new content – such as text, images, audio, or video – based on patterns learned from existing data.

(73) Generative Adversarial Network (GAN): A type of AI model that uses two neural networks—a generator and a discriminator—that compete with each other to create realistic synthetic data, such as images or videos.

(74) Generative Pretrained Transformer (GPT): A type of LLM designed to generate text by predicting the next word in a sequence, enabling tasks like conversation, summarisation, and content creation.

(75) 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.

(76) 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.

(77) Machine Learning (ML): A subset of AI where systems learn from data and improve their performance over time without being explicitly programmed.

(78) MetaData: MetaData is like labels on a file folder – helping everyone understand what's inside, how to use it, and where to find it.

(79) MetaData Management: Metadata Management is the practice of organising and maintaining this 'data about data' – capturing what it is, where it came from, how it’s structured, and how it should be used.

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

Status and Details

Status	Current
Effective Date	12th May 2026
Review Date	12th May 2029
Approval Authority	Vice-Chancellor
Approval Date	20th April 2026
Expiry Date	Not Applicable
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Tara Dharnikota Chief Information Security Officer Tara.Dharnikota@vu.edu.au
Enquiries Contact	Nea Dhillon Director, AI Technology & Delivery +61 3 9919 5894

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Victoria University's Policy Library for the latest version.