

ARTIFICIAL INTELLIGENCE(AI) USE POLICY AND PROCEDURE

1. Purpose

This Policy and Procedure establish how Training Masters will use Artificial Intelligence (AI) safely, ethically and transparently. It is intended to support innovation and efficiency while protecting the integrity of training and assessment, maintaining human accountability, safeguarding personal and confidential information, and ensuring fair outcomes for students.

The Policy provides clear requirements for the responsible use, monitoring and review of AI tools by staff, contractors and students.

2. Policy

Training Masters may use AI tools to support administration, learning resources, accessibility, quality assurance and service improvement. AI must support—not replace—professional judgement, qualified assessment decisions, compliance decisions or human accountability.

All AI-supported work must be checked by an appropriately responsible and qualified staff member before it is used or communicated. Training Masters will not use AI as the sole basis for any decision affecting a student, including assessment outcomes, support, reasonable adjustment, complaints, appeals, course progress, attendance, deferment, suspension, cancellation or visa-related matters.

AI must not be used in a way that compromises assessment authenticity, privacy, copyright, equity, accuracy, security or the requirements of a training product. Students must follow Training Masters' College AI requirements and complete the AI declaration for every assessment submission, whether or not AI was used.

3. Definitions

Term	Meaning
Artificial Intelligence (AI)	Technology capable of generating, analysing, summarising, translating, predicting or automating content or activities.
Generative AI	AI that creates text, images, audio, video, code or other content in response to prompts.
Public AI Tool	A publicly available or personal AI service. Personal, sensitive or confidential information must not be entered unless appropriate privacy and security safeguards are in place.
Human Oversight	Review by an appropriately qualified person who remains accountable for the final output or decision.
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable.
Confidential Information	Non-public student, staff, commercial, operational, assessment or third-party information held by Training Masters.
AI Misuse	Use of AI contrary to this Policy, assessment instructions, privacy obligations, academic integrity requirements or other College policies.

4. Responsibilities

Role	Responsibility
CEO	Approves this Policy, maintains overall accountability and decides serious AI-related incidents and risks.
Academic Manager	Oversees AI use in training and assessment; ensures human oversight, assessment integrity and training product alignment; coordinates AI risk review, staff guidance, incident response, monitoring and continuous improvement.
Trainers/Assessors	Explain the College AI requirements, ensure students complete the AI declaration, verify assessment authenticity, review AI-assisted materials and independently make assessment decisions.
Student Services and Administration	Use AI only for legitimate College purposes, protect student information, provide human support and maintain required records.
Marketing Staff	Ensure AI-assisted marketing is accurate, current, appropriately reviewed and not false or misleading.
All Staff and Contractors	Use AI responsibly, protect information, check outputs, keep required records and report misuse or incidents promptly.
Students	Follow the College AI requirements, submit authentic work, complete the AI declaration for every assessment submission and retain evidence of their work when requested.

5. Requirements

Training Masters will ensure that AI use is controlled, transparent and subject to human oversight. In particular:

- AI use must have a legitimate educational or operational purpose and be appropriate for the information and activity involved.
- Personal, sensitive or confidential information must not be entered into public AI tools or any system that does not provide appropriate privacy and security safeguards.
- AI outputs must be checked for accuracy, bias, relevance, copyright, currency and compliance before use.
- Staff remain responsible for all work produced with AI support.
- AI must not make assessment or other decisions affecting a student.
- Students must be informed of Training Masters' College AI requirements through orientation, the Student Handbook, AI Use in Learning and Assessment Reference Guide, LMS and Assessment Cover Sheet. Any assessment-specific conditions or restrictions must be communicated clearly and retained in writing.
- AI-detection and similarity results may be used as indicators only and must not be treated as proof of misconduct.
- AI-assisted assessment tools and learning resources must be reviewed against the current training product and student cohort before use.

These requirements support the Standards for RTOs 2025, including Standards 1.3, 1.4 and 1.5 in relation to assessment tools, the Principles of Assessment, Rules of Evidence and validation. AI-related risks and improvements will also be managed through Training Masters' risk management and continuous improvement processes.

6. Scope

This Policy applies to all Training Masters students, employees, trainers and assessors, managers, contractors, consultants, education agents and third-party providers who use AI in connection with college operations, services, learning or assessment.

It applies to generative AI, chatbots, automated content or analytics tools, AI features embedded in software, transcription and translation tools, and plagiarism or AI-detection services.

7. Procedures

7.1 Permitted Organisational and Staff AI Use

Subject to privacy, confidentiality, security and human-review requirements, Training Masters staff may use AI to assist with:

- drafting generic emails, templates, checklists and internal working documents;
- summarising public or non-confidential information;
- developing draft learning examples, scenarios and accessibility supports;
- grammar, clarity, formatting, captions, translation or plain-English support;
- administrative workflow and quality-assurance activities; and
- academic integrity screening where results are treated only as indicators.

7.2 Prohibited AI Use

AI must not be used to:

- enter names, USIs, dates of birth, contact details, results, attendance, course progress, visa information, complaints, welfare or medical information, payment information or staff records into public AI tools or systems without appropriate privacy and security safeguards;
- make Competent or Not Yet Competent decisions or replace assessor judgement;
- make decisions about support, reasonable adjustment, complaints, appeals, welfare, enrolment, deferment, suspension, cancellation or visa matters;
- fabricate assessment evidence, workplace evidence, observations, reports, references, logbooks, signatures, images or records;
- produce misleading marketing, false claims or inaccurate regulatory information;
- hide plagiarism or prohibited AI use through humanising or paraphrasing tools; or
- upload confidential Training Masters or third-party documents contrary to privacy, confidentiality or information-security requirements.

7.3 AI Use in Learning and Assessment

Students may use AI tools for limited learning and assessment support in accordance with this Policy, including the acceptable-use requirements and mandatory AI declaration.

Acceptable AI use includes:

- brainstorming and developing ideas;
- explaining difficult concepts;
- identifying research topics or keywords;
- creating practice questions for personal study;
- planning the structure of a response;
- checking basic spelling, punctuation and grammar; and
- receiving general feedback that the student reviews and applies independently.

AI must support the student's learning and must not generate, complete or substantially rewrite assessment responses. Students must prepare the final response in their own words and demonstrate their own knowledge, skills and understanding.

Students must complete the AI declaration for every assessment submission, confirming whether AI was used. Where AI was used, the student must identify the tool and explain how it assisted them.

AI-generated or AI-rewritten assessment responses, fabricated evidence, false references or undeclared AI use are prohibited and may be treated as academic misconduct.

Where an assessment is specifically designed to assess the use of AI, the assessment instructions may permit additional uses and must clearly explain the permitted use and evidence requirements. The requirements of this Policy, the AI Use in Learning and Assessment Reference Guide and the Assessment Cover Sheet apply to all assessments.

7.4 Privacy, Confidentiality and Security

Staff must use generic or de-identified information wherever possible, such as “Student A”, “Trainer B” or “Course X”. De-identification must be effective; removing a name alone may not be sufficient if other details can identify the person.

Personal or confidential information may only be processed through a system with appropriate privacy and security safeguards, for a legitimate College purpose and in accordance with Training Masters’ privacy, information-security and recordkeeping requirements. AI prompts and outputs containing College information are College records where they form part of a decision, service, assessment process or compliance activity.

7.5 Human Review, Transparency and Student Rights

All AI-assisted content must be reviewed by the staff member responsible for the work before use. That person remains accountable for checking its accuracy, suitability, bias, currency, copyright and compliance. High-risk, assessment-related or regulatory content must be referred to the Academic Manager or CEO where appropriate.

Students will be informed about relevant AI use through orientation, assessment instructions, the Student Handbook and other appropriate communication. A student may ask how AI was used in a process affecting them and may request human review. Where reasonable and practicable, Training Masters will provide a non-AI or human-supported pathway.

7.6 AI Incident and Breach Response

Step 1: Any suspected misuse, inaccurate output, improper disclosure, security issue or privacy incident must be reported immediately to the Academic Manager and no later than 24 hours after discovery.

Step 2: The affected use or tool must be stopped where necessary, available evidence preserved and immediate action taken to contain or reduce harm.

Step 3: The Academic Manager records and assesses the incident, notifies the CEO and relevant manager, and determines corrective action.

Step 4: Where personal information is involved, Training Masters will assess the incident under its Privacy Policy and the Notifiable Data Breaches scheme, including whether notification to the Office of the Australian Information Commissioner and affected individuals is required.

Step 5: The outcome, corrective actions and any required improvements are recorded in the relevant incident, risk and continuous improvement records.

7.7 Training, Monitoring and Records

Staff will receive AI awareness training at induction, when AI tools or requirements materially change, and through ongoing professional development. Training will address responsible and prohibited uses, privacy, assessment integrity, human oversight, verification and incident reporting.

Training Masters will maintain records appropriate to the risk and use, including AI risk reviews, staff training, material AI use, student declarations, integrity investigations, incidents, complaints, validation and continuous improvement. Records will be stored securely and accessed only by staff with a legitimate business need.

7.8 Related Policies and Documents

This Policy should be read together with the Plagiarism and Academic Misconduct Policy and Procedure; Assessment Policy and Procedure; Privacy Policy; Records Management Policy;

Complaints and Appeals Policy and Procedure; Student Code of Conduct; Staff Code of Conduct; Student Handbook; Risk Management Policy; and Continuous Improvement Policy and Procedure.

8. Implementation

This Policy will be implemented through staff induction and professional development, student orientation, College- AI guidance, student declarations, risk-based controls, internal monitoring, validation, privacy and security controls, and audit activities. Managers are responsible for ensuring that staff and contractors understand and apply the requirements relevant to their roles.

9. Review and Continuous Improvement

This Policy and Procedure will be reviewed at least annually, or earlier where legislation, regulatory guidance, technology, vendor terms, operational arrangements or risks change. It will also be reviewed following an AI-related incident, complaint, appeal, validation finding, audit finding or significant new use of AI.

Feedback and review outcomes will be analysed and approved improvements will be recorded in the Continuous Improvement Register, implemented through Training Masters' quality assurance processes and communicated to relevant stakeholders.