

ARTIFICIAL INTELLIGENCE (AI) POLICY & PROCEDURE

Introduction

The Artificial Intelligence (AI) Use Policy and Procedure is a critical component of King's Own International College (KOIC)'s governance, academic integrity, privacy, and quality assurance framework. It establishes the principles, expectations, and controls for the ethical, transparent, and responsible use of Artificial Intelligence technologies across academic, operational, and administrative functions.

KOIC recognises that AI technologies are rapidly evolving and increasingly integrated into education, industry, and workplace environments. AI tools can support innovation, accessibility, operational efficiency, student engagement, and personalised learning experiences. At the same time, inappropriate or uncontrolled use of AI may create risks relating to academic integrity, privacy breaches, misinformation, bias, intellectual property, assessment authenticity, cybersecurity, and regulatory non-compliance.

KOIC is committed to ensuring that AI is used in a manner that supports, rather than replaces, professional judgement, educational integrity, and human oversight. AI systems must not compromise the validity of assessment, the authenticity of student work, the confidentiality of personal information or the integrity of nationally recognised training outcomes.

This Policy and Procedure aligns with:

- Standards for Registered Training Organisations (RTOs) 2025
- ESOS Act 2000
- National Code 2018
- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- Student Identifiers Act 2014
- ASQA guidance relating to generative AI and assessment integrity
- KOIC Privacy and Data Use Policy & Procedure

This policy supports KOIC's commitment to ethical governance, academic integrity, risk management, and student-centred practice.

Purpose

The purpose of this policy is to:

- establish clear expectations for the appropriate use of AI technologies at KOIC;
- protect academic integrity and assessment authenticity;
- ensure compliance with privacy, confidentiality, and cybersecurity obligations;
- support ethical, transparent, and responsible AI use;
- define acceptable and prohibited uses of AI by staff;
- ensure AI supports rather than replaces professional judgement;
- protect student, staff, and organisational data;
- support innovation while managing associated risks.

Scope

This policy applies to all KOIC employees, trainers and assessors, ELICOS teachers, contractors and consultants and third-party providers acting on behalf of KOIC.

This policy applies to all AI technologies, including:

- generative AI tools;
- AI writing assistants;
- AI chatbots;
- AI image, audio, and video generators;
- AI transcription and translation tools;
- automated marking or analytics systems;
- AI-powered learning platforms;
- AI productivity software integrated into workplace systems.

Policy Statement

King's Own International College (KOIC) recognises that Artificial Intelligence (AI) technologies are becoming increasingly integrated into education, administration and industry practices. KOIC supports the responsible and ethical use of AI, where it enhances learning, accessibility, operational efficiency and student support while maintaining academic integrity, privacy, human oversight and regulatory compliance.

KOIC acknowledges that AI can provide significant educational benefits, particularly in supporting personalised learning, improving accessibility for students requiring reasonable adjustments, assisting students with language or literacy needs, and preparing graduates for modern workplaces where AI technologies are increasingly utilised. AI tools may also support administrative efficiency and reduce repetitive operational tasks.

However, AI technologies also present risks relating to privacy, confidentiality, academic integrity, misinformation, cybersecurity, bias, intellectual property and the authenticity of assessment evidence. KOIC is committed to ensuring that AI is used ethically, transparently and responsibly and that it does not compromise the integrity of training and assessment outcomes or the obligations of staff under the Standards for RTOs 2025, ESOS legislation and privacy laws.

AI must support, rather than replace, professional judgement. Final decisions relating to competency, assessment outcomes, student progression, compliance, academic integrity matters and regulatory obligations must always involve qualified staff exercising independent professional judgement.

Staff remain accountable for all work produced using AI technologies. AI-generated outputs must be reviewed for factual accuracy, contextual appropriateness, bias, compliance requirements and privacy considerations prior to use. Staff must not rely solely on AI-generated information without verification.

KOIC maintains transparency regarding organisational use of AI technologies and may disclose the use of AI systems where relevant to educational delivery, assessment, student support or operational processes.

Definitions

Artificial Intelligence (AI)	Computer systems capable of performing tasks that normally require human intelligence, including generating text, images, audio, analysis, or predictions.
Generative AI	AI systems capable of creating new content such as written text, images, video, code, or audio.
Personal Information	Information or opinions about an identifiable individual as defined under the Privacy Act 1988 (Cth).

Sensitive Information	Information relating to health, ethnicity, visa status, criminal history, biometric information, or other protected information under privacy legislation.
Human Oversight	Review, verification and approval by a qualified staff member prior to implementation or reliance on AI-generated outputs.
Academic Integrity	Honest, ethical, and authentic participation in learning, assessment, and educational processes.

Regulatory and Legislative Requirements

- Standards for RTOs 2025
- ESOS Act 2000
- National Code 2018
- Privacy Act 1988 (Cth)
- Australian Privacy Principles (APPs)
- Student Identifiers Act 2014
- Data Provision Requirements 2020
- NVR Act 2011

Artificial Intelligence (AI) Procedure

1. Appropriate Use of AI

KOIC permits the use of approved AI tools where the use is lawful, ethical, proportionate and aligned with educational and operational objectives.

AI may be appropriately used to assist with drafting communications, improving grammar and readability, summarising information, supporting lesson planning, developing draft learning activities, generating ideas, preparing non-regulatory administrative documents and improving accessibility for students requiring additional support.

AI may also be used to support students with language, literacy or accessibility needs, including tools that convert written information into audio, provide translation assistance or support comprehension through simplified explanations.

Where AI is used within training and assessment practices, it must support learning rather than replace authentic student work. Staff must ensure students continue to demonstrate genuine competency through valid assessment methods including practical demonstration, workplace tasks, projects, oral questioning, direct observation and other authentic evidence-gathering approaches.

KOIC recognises ASQA guidance that AI may assist with educational delivery and operational efficiency, but it must not undermine the integrity of competency-based assessment or replace the professional judgement of qualified assessors.

2. Prohibited Use of AI

AI must not be used in any way that compromises academic integrity, assessment authenticity, privacy obligations,

compliance requirements or organisational integrity.

Staff must not use AI to generate or alter student assessment evidence, fabricate workplace documentation, create false records, produce fraudulent attendance or assessment outcomes, or generate evidence that falsely represents student competency.

AI must not independently determine competency outcomes or replace assessor judgement. Automated tools may assist with administrative processes such as quiz marking or preliminary analysis, however final assessment decisions and feedback must always be reviewed and confirmed by a qualified assessor.

Staff must not use AI to generate misleading governance records, validation outcomes, industry consultation evidence, audit documentation or compliance evidence. All compliance and governance documentation must accurately reflect genuine activities and decisions.

AI must not be used to create discriminatory, offensive, defamatory, deceptive or harmful content, or to impersonate another individual or organisation.

3. Assessment Integrity and Human Oversight

KOIC is committed to ensuring that all assessment practices continue to meet the Principles of Assessment and Rules of Evidence in the age of AI.

Assessment decisions must always be based on evidence of the individual learner's own performance. AI-generated responses or AI-assisted work must not replace genuine demonstrations of competency.

Assessors are required to apply professional judgement and implement appropriate assessment methods to confirm authenticity. This may include oral questioning, live demonstrations, workplace observation, scenario-based assessment activities, and other methods that verify the student's understanding and capability.

Assessors must ensure that:

- assessment evidence remains authentic, valid, current, and sufficient;
- students can independently explain and apply their knowledge and skills;
- assessment methods reflect current industry practice;
- students are provided with personalised feedback;
- academic integrity concerns relating to AI are identified and managed appropriately according to KOIC's Academic Integrity Policy.

Where concerns arise regarding inappropriate AI use, staff must follow KOIC's academic integrity and misconduct procedures.

KOIC acknowledges that AI detection technologies may produce unreliable or false-positive results. AI detection tools may be used as one indicator only and must not be solely relied upon when determining academic misconduct, assessment authenticity concerns or breaches of academic integrity. Professional judgement, supporting evidence and direct student engagement must also be considered.

4. Privacy, Confidentiality and Data Security

All staff must comply with the KOIC Privacy and Data Use Policy & Procedure when using AI technologies.

Due to the nature of many public AI platforms, staff must exercise extreme caution when entering information into AI systems. Many AI tools store, analyse or reuse uploaded content, creating significant privacy and confidentiality risks.

Staff must not upload, enter, or share confidential, personal, or sensitive information into public or unapproved AI platforms. This includes:

- student personal information;
- passport or visa documentation;
- USI details;
- medical or wellbeing information;
- student assessment evidence;
- complaints or appeals information;
- staff employment records;
- commercially sensitive information;
- audit reports or regulatory correspondence;
- confidential governance or financial records.

Where AI tools are approved for organisational use, staff must use de-identified or anonymised information wherever possible.

KOIC maintains an AI Systems Register which identifies approved AI technologies, permitted uses, associated risks, privacy considerations, human oversight controls and review requirements. KOIC may approve, restrict or prohibit the use of specific AI platforms based on privacy, cybersecurity, confidentiality, operational or regulatory risks. Staff must only use AI systems that have been authorised for organisational use where applicable. Refer to **Appendix 1 – AI Systems Overview** which identifies approved AI technologies.

Staff should be aware that some AI systems store or process information outside Australia. AI tools must not be used in a manner that breaches privacy legislation, confidentiality obligations, contractual requirements or KOIC's data governance requirements.

All staff are responsible for protecting confidentiality, maintaining cybersecurity awareness, and ensuring AI use aligns with the Privacy Act 1988 (Cth), Australian Privacy Principles and KOIC's internal privacy and data governance requirements.

5. Ethical Use and Professional Responsibility

All staff are expected to use AI ethically, responsibly and transparently. AI should enhance professional practice rather than diminish critical thinking, professional judgement or educational quality.

Staff must critically evaluate AI-generated outputs and recognise that AI systems may produce inaccurate, biased, outdated or fabricated information. AI-generated content must not be accepted at face value.

Staff must also ensure that AI-generated materials do not breach copyright, licensing, attribution or intellectual property obligations. Any materials generated or adapted using AI must be reviewed to ensure lawful, ethical and

appropriate use.

Staff are responsible for ensuring that any materials developed using AI are accurate, appropriate, inclusive, compliant and aligned with KOIC's educational standards and regulatory obligations.

KOIC will monitor AI use to minimise risks of bias, discrimination or inequitable impact on students or staff.

Where AI materially contributes to operational, educational or administrative content, staff should maintain transparency regarding its use where appropriate.

Staff must ensure there is appropriate transparency where AI has materially contributed to the development of learning resources, assessment tools, operational documentation or compliance-related materials. Staff may be required to retain evidence of review, editing and human oversight processes to demonstrate accountability and authenticity.

Procedure Summary Table

Step	Action	Responsible	Timeframe	Record/Reference
1	Staff complete AI awareness and cybersecurity training	CEO / Compliance Officer	On commencement and annually	PD Records
2	Approved AI tools reviewed and authorised	CEO / IT / Compliance	As required	AI Systems Register
3	Staff use AI in accordance with policy	All Staff	Ongoing	Internal Systems
4	Sensitive or confidential information restricted from AI upload	All Staff	Ongoing	Privacy Procedures
5	Assessment decisions reviewed by qualified assessors	Trainers / Assessors	Ongoing	Assessment Records
6	AI-related concerns or breaches reported	All Staff	As identified	Incident Register
7	AI-related risks reviewed through continuous improvement processes	Compliance Officer	Quarterly	Continuous Improvement Registers
8	Policy reviewed against emerging regulatory guidance	CEO / Compliance Officer	Annually	Policy Review Record
9	Staff complete AI and Academic Integrity Declaration	All Staff / Compliance Officer	On commencement and annually	AI and Academic Integrity Declaration Form

Roles and Responsibilities

Role	Responsibility
CEO	is responsible for overall oversight of AI governance, implementation, and compliance monitoring within KOIC.

Compliance Officer	is responsible for monitoring AI-related compliance risks, reviewing emerging regulatory guidance and supporting implementation of this policy.
Teachers, Trainers, and Assessors	are responsible for ensuring AI is used appropriately within their areas of responsibility and that assessment integrity and human oversight are always maintained.
All staff	are responsible for complying with this policy, protecting confidentiality, and reporting any suspected misuse of AI technologies.
IT team (Shared Service)	is responsible for monitoring cybersecurity risks, approved systems and digital safeguards relating to AI technologies.

Policy Implementation

KOIC is committed to implementing this policy through staff awareness, training, governance oversight and continuous monitoring of emerging AI-related risks and regulatory expectations.

- This policy will be made available to all staff members and relevant stakeholders through internal communication systems, induction processes, staff handbooks, and policy repositories. Relevant elements of AI governance and academic integrity expectations will also be communicated to students through orientation, student handbooks, assessment instructions, and academic integrity processes.
- All staff involved in training, assessment, compliance, administration, or student support will receive guidance and professional development relating to:
 - ethical and appropriate use of AI technologies;
 - academic integrity and assessment authenticity;
 - privacy, confidentiality, and cybersecurity obligations;
 - human oversight requirements;
 - risks associated with public AI platforms;
 - emerging regulatory expectations and sector guidance.
- Staff are also required to complete an AI and Academic Integrity Staff Declaration on induction and annually thereafter to acknowledge their understanding of approved AI use, confidentiality obligations, academic integrity requirements, human oversight expectations and professional responsibilities relating to AI technologies.

KOIC will maintain oversight of approved AI tools and may restrict or prohibit the use of specific AI platforms where privacy, cybersecurity, confidentiality, or operational risks are identified.

The use of AI within training, assessment and operational practices will be monitored through internal audits, validation activities, assessment reviews, continuous improvement processes, and compliance monitoring activities to ensure ongoing alignment with the Standards for RTOs 2025 and applicable legislative requirements.

Where AI-related risks, incidents or breaches are identified, corrective action and continuous improvement measures will be implemented and documented within KOIC's Continuous Improvement Register.

Monitoring and Review

KOIC will regularly monitor the use of AI technologies through internal audits, assessment validation activities,

[Australian Academy of Commerce Pty Ltd trading as King's Own International College](#)

ABN 97 107 328 478

RTO 90982 | CRICOS 02599C

KOIC Artificial Intelligence (AI) Policy V1.0 2026

compliance reviews, staff declarations, staff feedback, cybersecurity monitoring and continuous improvement processes.

AI-related risks, incidents or emerging issues will be recorded and managed through the Continuous Improvement Register where appropriate.

This policy will be reviewed every two years, or earlier if required, to reflect changes in legislation, regulatory expectations, technology developments or organisational operations.

Version Control

Version	Date	Description	Approved by	Approval date	Author	Review date
V1.0	May 2026	New AI Policy implemented for KOIC	CEO	04 August 2026	Compliance Officer	Aug 2028

Policy and Document Information

Author:	Compliance Officer
Policy owner:	Compliance Officer
Approved by:	CEO
Approved date:	04 August 2026
Status:	Approved
Next review due:	Aug 2028

Appendix 1 – Approved AI Systems Overview

KOIC maintains an AI Systems Register to support governance, risk management, privacy protection, and responsible use of Artificial Intelligence technologies across educational, operational, and administrative activities.

Approved AI systems may be used for purposes including:

AI Tool	Approved Use
Adobe Firefly	Graphic design and branded content development
AI Translation Tools	Language support for students and staff communication
Canva AI Tools	Draft visual design and marketing support
Canva AI Image Tools	Marketing graphics, social media content, promotional materials, and visual concept development
DALL-E / ChatGPT Image Generation	Draft visual concepts, promotional imagery, and creative design support
ChatGPT (Public Version)	Drafting ideas, grammar support, summarising non-confidential information, lesson planning support
Claude (Anthropic)	Drafting content, summarising information, brainstorming, policy drafting support, learning resource development and administrative assistance
Grammarly AI	Grammar, readability, and language support
Microsoft Copilot	Administrative drafting, meeting summaries, internal productivity support within approved systems
Otter.ai / AI Transcription Tools	Meeting transcription and note generation
Turnitin / Copyleaks	Similarity checking and assessment authenticity review
ZeroGPT / AI Detection Tools	Preliminary AI-content risk indication only

All approved AI systems are subject to risk assessment, human oversight, and periodic review. Risk levels vary depending on the nature of the AI system, the type of data processed and the operational context.

Please refer to KOIC's AI Systems Register.