

Department	Vocational Education & Training	
Quality Controlled Document No. & Title	2026-08-11	AI Policy
Version	2.1	
SRTOs 2025 ESOS National Code 2018 ELICOS Standards 2018	Standards 4.1 – 4.4 N/A N/A	



Author	RTO Manager	
Approved	CEO	
Authorised	CEO	
Distribution	Internal	Staff Students
	External	Prospective Students

1.0 Policy Scope

1.1 This policy applies to all AI use connected with the Institute, including public generative AI tools, enterprise AI tools, AI built into the learning management system, plagiarism or authorship tools, proctoring tools, transcription or meeting-summary tools, chatbots, adaptive learning tools, image/audio/video/code generators, translation tools, data analytics and automated workflow tools.

1.2 The policy applies across nationally recognised training, non-accredited training, online delivery, classroom delivery, blended delivery, workplace learning, placement, marketing, enrolment, student support, resource development, assessment, validation and administration. Where a third party acts for St Peter Institute, the third party must comply with this policy and any stricter contract or regulatory requirement.

1.3 This policy supports compliance with the Standards for RTOs 2025, including the Outcome Standards and section 20 (Governance) of the Compliance Requirements, the National Vocational Education and Training Regulator Act 2011 (Cth), the Privacy Act 1988 (Cth) and the ESOS framework, and is informed by ASQA's draft AI Principles for the responsible use of AI in VET delivery.

1.4 Related documents: Academic Integrity Policy, Complaints and Appeals Policy, Privacy Policy, Records Management Policy, Student Handbook, Staff Handbook, Training and Assessment Strategies, and assessment cover sheets and declarations.

2.0 Definitions

Term	Meaning for this policy
AI	A technology or system that performs tasks normally requiring human judgement, reasoning, prediction, classification, language generation, image generation or decision support.
Generative AI	AI that creates or transforms content such as text, code, images, audio, video, summaries, feedback, translations, data analysis or lesson materials.
Public AI tool	A generally available AI tool accessed through a public website, app or individual account, where inputs or outputs may be stored or used by the provider unless settings and terms say otherwise.
Approved AI tool	A tool assessed and approved by the CEO, or delegate, for a defined purpose, risk level, data type and user group.
AI-assisted work	Work where AI helped with ideas, planning, editing, language support, summarising, formatting, practice or feedback, but the student or staff member remains responsible for the final content.
AI-generated assessment evidence	Assessment material generated wholly or substantially by AI instead of demonstrating the student's own knowledge, skills and performance. This is not acceptable evidence unless the task explicitly requires AI use and assesses the student's use, critique and application of AI.
Elevated-risk AI use	AI use that involves personal or sensitive information, student records, assessment decisions, profiling, proctoring, high-stakes support, automated decision-making, substantial impact on a student, third-party data sharing, or reputational/safety risk.

3.0 Policy Principles

3.1 Student learning first: AI is used to deepen understanding, feedback and capability, not to bypass learning or assessment.

3.2 Human accountability: a staff member remains responsible for any AI-assisted resource, communication, support action or decision. AI cannot make final assessment or certification decisions.

3.3 Assessment integrity: evidence must remain valid, sufficient, authentic and current. Students must demonstrate competence through their own work and performance.

3.4 Transparency and disclosure: students and staff must know when AI is permitted, when it is prohibited, and when AI use must be acknowledged.

3.5 Privacy and data minimisation: personal, sensitive, confidential, assessment, commercial and workplace information is not entered into public AI tools.

3.6 Fairness, equity and accessibility: AI controls must not disadvantage students because of disability, language background, device access, digital capability or location. Reasonable adjustment remains available.

- 3.7 Safety, reliability and verification: AI outputs must be checked against authoritative sources, training package requirements, legislation, industry practice and the RTO's approved resources before use.
- 3.8 Contestability: students and staff can ask how AI was used in a decision or process and can challenge suspected AI misuse or AI-supported decisions under the complaints and appeals process.
- 3.9 Continuous improvement: AI risks, incidents, audit findings, validation outcomes and stakeholder feedback are monitored and used to improve the policy and assessment system.

4.0 Governance and Accountability

St Peter Institute will manage AI through documented governance controls proportionate to the risk of the use case. AI governance sits within the RTO quality framework, continuous improvement process and assessment validation system.

Role	Responsibilities
CEO	Approves this policy, ensures resources for safe implementation, receives reports on elevated-risk AI use, privacy incidents, assessment-integrity trends and corrective actions.
RTO Manager	Approves the use case for AI use and documents the controls. Ensures assessment systems and practices include authenticity controls and practical evidence; supervises trainer implementation; schedules validation and standardisation activities. Maintains the AI Tool Register and AI Use Case Register; approves or rejects AI tools; completes risk assessments; coordinates privacy checks; maintains policy currency; reports to management.
Trainers and Assessors	Teach permitted AI use, protect information, record AI-assisted resource development, validate outputs, apply assessment instructions, collect authentic evidence and make independent judgement of competency.
Student Support / Administration	Use AI only for approved support and communication tasks, verify content before sending, protect student information and escalate risks or incidents.
Students	Use AI only as permitted for each task, disclose AI assistance where required, protect personal/workplace information, verify AI output and submit their own work and performance evidence.
Third parties and contractors	Comply with this policy and associated procedures, privacy/security requirements and contractual controls. They must not use student or Institute information in AI tools without written approval.

5.0 AI Approval and Risk Controls

- 5.1 Before any AI tool or elevated-risk AI use is implemented, the RTO Manager, as the CEO's delegate, must approve the use. Approval must be limited to the specific purpose, user group and data type assessed. Approval for one use case does not authorise use for assessment judgement, student profiling or unrelated data handling.
- 5.2 The Institute shall maintain an AI Tool Register recording tool name, owner, purpose, approved users, approved data types, privacy/security review, risk rating, expiry/review date and conditions of use.
- 5.3 The RTO Manager, in consultation with stakeholders, shall conduct an AI risk assessment before using AI for assessment design, student-facing support, decision support, automated communications, proctoring, authorship detection, transcription, analytics or any use involving personal information.
- 5.4 The RTO Manager shall complete a Privacy Impact Review where personal information, sensitive information, biometrics, student records, workplace evidence or automated decision-making is involved.
- 5.5 The RTO Manager shall maintain an AI Use Case Register for AI uses in assessment, student support, administration, marketing, resource development, analytics or quality assurance.
- 5.6 The Institute shall ensure that approved AI tools are reviewed at least annually and after significant product, terms of service, privacy, security or functionality changes. Reports shall be tabled at Management Team meetings.

6.0 Prohibited and high-control AI uses

Category	Rules
Prohibited for all users	• Entering student personal information, sensitive information, student identifiers, assessment records, complaints, support notes, health/disability information, financial information or workplace/client information into public AI tools. • Uploading copyrighted third-party resources, textbooks, commercial assessment tools, Institute templates or student submissions into public AI tools unless the licence and Institute approval expressly permit it. • Using AI to impersonate a student, trainer, employer, workplace supervisor, referee or Institute representative. • Creating misleading evidence, fabricated logs, fake references, fabricated workplace documents, deepfakes or false declarations. • Allowing AI to make final assessment, grading, credit, RPL, admission, exclusion, certification, complaint, appeal or disciplinary decisions.
High-control uses requiring written approval	• AI-supported proctoring, identity verification, authorship detection or plagiarism detection. • AI chatbots or automated messages that provide student-facing information about enrolment, fees, progression, assessment, visas, complaints or support. • AI analytics used to identify at-risk students or trigger intervention. • AI-assisted transcription, note-taking or summarising of meetings involving students, staff performance, complaints, assessment, sensitive matters or commercially confidential information. • Any AI use involving children, vulnerable cohorts, disability support records, workplace placement evidence, biometrics, health information or external client data.

7.0 Student AI Use Rules

7.1 Students may use AI as a learning aid where the assessment instructions permit it. Unless an assessment task states otherwise, students may use AI to explain concepts, create study plans, generate practice questions, brainstorm approaches, check grammar, improve plain English, translate short non-assessment phrases for comprehension, organise notes, or ask for feedback on clarity. Students must still verify the output and submit their own work.

7.2 Students must not use AI to produce final assessment answers, practical evidence, workplace evidence, reflective journals, logbooks, supervisor reports, observations or declarations unless the task explicitly permits AI use and the student discloses it. AI-generated content is not automatically authentic assessment evidence. The student must be able to explain and demonstrate the knowledge and skills claimed in their submission.

8.0 Student Assessment AI Permission Categories

Category	Meaning	Evidence/statement required
Red - No AI permitted	AI must not be used for any part of the task except ordinary spelling and/or grammar tools expressly allowed by the assessor. Suitable for closed-book tests, safety-critical skills, practical observation, identity-controlled tasks or tasks where unaided performance is required.	Student declaration: "I did not use AI for this assessment except permitted spelling/grammar tools."

Amber - AI for learning support only	AI may be used for understanding concepts, planning, practice, language support or feedback. It must not be used to generate final answers or evidence. Student must retain drafts/notes if requested.	Student declaration: "I used AI only for permitted study or editing support and the final work is my own."
Green - AI-assisted work permitted with disclosure	AI may assist with drafting, structure, examples, analysis or coding where the task is designed to assess critical use of AI and the student's judgement. The student must disclose the tool, purpose and how outputs were checked.	Student declaration and an AI acknowledgement table required.
Blue - AI-integrated task	AI use is a required component of the assessment. The task assesses design, evaluation, verification, bias and risk analysis, application to workplace context and reflection. The student must provide process evidence.	Student submits prompts and output samples, critique, verification sources and final human-refined product.

9.0 Student AI Management Strategies

Strategy for students	Implementation requirement	Evidence
Student AI induction module	All new students complete a short module before first assessment. Content covers what AI is, permitted/prohibited use, privacy, copyright, hallucinations, bias, disclosure, assessment authenticity and consequences of misuse.	Completion recorded in LMS or student management system; quiz result and signed declaration retained.
Assessment-specific instructions	AI Every assessment task is labelled Red, Amber, Green or Blue. Instructions explain examples of allowed AI use, prohibited use, disclosure requirements and authenticity evidence required.	Assessment tool review checklist; sample audit of issued assessment tasks.
Student AI declaration	Each assessment submission requires a declaration confirming whether AI was used and whether the work is the student's own. Green and Blue tasks require the AI acknowledgement template.	Submission cover sheet or LMS declaration retained with assessment record.
AI acknowledgement template	Students record tool name, date, purpose, prompt summary, output used, verification method and changes made. Students do not need to provide private account details or full prompts containing personal information.	Acknowledgement template stored with assessment submission.
Practical AI literacy activities	Trainers teach students how to test AI outputs, find errors, check against reliable sources, identify bias, protect privacy and cite or acknowledge AI assistance.	Session plan, learning activity, student sample or attendance record.
Authenticity interviews and oral questioning	Where risk indicators arise, the assessor conducts oral questioning, practical demonstration, knowledge checks or an authenticity interview before making judgement.	Questioning record, assessor notes, recording if permitted, and outcome retained.

Process evidence for vulnerable tasks	For take-home written tasks or projects, students may be asked for outlines, drafts, version history, screenshots, calculations, practical artefacts, research notes or reflective logs.	Process evidence linked to assessment record.
Access and equity controls	Students without reliable AI access are not disadvantaged. Where AI use is required, the RTO provides approved access or an equivalent alternative. Reasonable adjustment is available where AI or non-AI requirements affect disability, LLN or digital access.	Support notes, reasonable adjustment record and assessment adjustment approval where relevant.
Privacy and workplace safety rules	Students are explicitly told not to enter names, contact details, employer/client information, health information, workplace records, placement evidence or other personal/confidential information into public AI tools.	Student handbook, induction module and assessment instructions.
Support before misconduct	Where a student is unsure about permitted AI use, trainers provide guidance before submission. Suspected misuse is handled fairly, with an opportunity for the student to respond and demonstrate competence.	Support records, authenticity interview, reassessment plan or misconduct outcome.

10.0 Trainer AI Use Rules

10.1 Trainers and assessors may use AI to support resource development, lesson planning, formative learning activities, plain-language explanations, accessibility, examples, scenarios, practice quizzes, industry research prompts and administrative drafting. AI output must be treated as an unverified draft. It must be checked before use against the training product, unit requirements, current industry practice, the training and assessment strategy, assessment conditions, workplace safety requirements, copyright obligations and the RTO's approved materials.

10.2 Assessors must not use AI to make final competency judgements or automatically accept, reject or score assessment evidence. AI tools, including AI detectors and plagiarism tools, may be used only as one risk indicator. Assessment decisions must be based on the evidence before the assessor and the principles of assessment and rules of evidence.

11.0 Acceptable AI Use for Trainers

11.1 Drafting lesson/session plans, classroom activities, formative quizzes, discussion prompts and examples, then validating them against the relevant unit and approved TAS.

11.2 Generating plain-English explanations, glossary items and alternative examples to support students with different LLN levels or learning needs.

11.3 Creating first-draft workplace scenarios or roleplays, provided they are contextualised to the RTO cohort, industry practice and assessment requirements before use.

11.4 Drafting feedback templates for formative learning, provided the trainer personalises and verifies feedback before giving it to students.

11.5 Summarising publicly available regulatory or industry information for trainer preparation, provided original authoritative sources are checked and cited in resources where appropriate.

11.6 Generating ideas for reasonable adjustment approaches, accessibility supports or learning scaffolds, subject to privacy, equity and assessment-integrity review.

12.0 Trainer and assessor strategies the RTOs will implement

Strategy for trainers/assessors	Implementation requirement	Evidence the RTO will keep
Mandatory trainer AI professional development	All trainers, assessors and relevant support staff complete AI literacy training before using AI for RTO purposes and then annually. Training covers AI limitations, hallucinations, bias, privacy, copyright, assessment authenticity, approved tools, traffic-light assessment categories, student support and incident escalation.	Trainer PD register, induction checklist, annual refresher completion and meeting minutes.
Assessment vulnerability review	Each unit/cluster is reviewed for AI vulnerability. High-risk written or take-home tasks are redesigned to include practical demonstration, observation, oral questioning, version history, student reflection, contextualisation or supervised components.	AI assessment risk matrix, updated assessment tools and validation records.
Assessment instruction uplift	Trainers ensure every task tells students the AI category, permitted and prohibited AI uses, required declaration, authenticity evidence, privacy warning and consequences of misuse.	Assessment tool checklist and trainer sign-off prior to issue.
Trainer AI use log	Where AI materially assists a learning resource, assessment draft, student communication template, marking guide or policy draft, the trainer records tool name, purpose, prompt summary, output used, verification and approval status.	Trainer AI Use Log retained by the RTO Manager.
Human verification and source checking	Trainers must verify AI outputs against authoritative sources, training package requirements, legislation, RTO policy and industry practice. Unverified AI outputs cannot be published, taught, assessed or sent to students.	Resource approval record, source list, version control and trainer notes.
Standardisation meetings	Trainer teams discuss AI-related assessment risks, benchmark evidence, suspected misuse patterns, reasonable adjustment examples and consistent application of AI categories.	Standardisation meeting agenda, minutes and actions.
Validation includes AI controls	Validation samples check whether assessment evidence remains valid, sufficient, authentic and current in light of AI. Validation considers student declarations, process evidence, oral questions, practical observation and assessor decision-making.	Validation plan, validation tools, completed validation reports and continuous improvement actions.

No sole reliance on AI detection	AI detectors are not used as decisive evidence of misconduct. Assessors must triangulate with assessment quality, version/process evidence, questioning, practical demonstration and student explanation.	Academic integrity case file showing all evidence considered.
Student coaching on ethical AI	Trainers explicitly teach how to use AI ethically within the discipline or workplace, including prompt design, verification, bias checks, privacy, copyright, work health and safety and professional responsibility.	Session plans, teaching resources and LMS announcements.
Protected information controls	Trainers must not paste student submissions, student data, assessment records, employer/client information or confidential RTO materials into public AI tools. Approved enterprise tools may only use the minimum data necessary and only for approved purposes.	Tool approval conditions, privacy training record and incident log where relevant.

13.0 Assessment Integrity Controls

13.1 St Peter Institute will not attempt to manage AI risk solely through detection software. The primary controls include Student English Proficiency Tasks administered prior to course commencement. These may then be used as a benchmark when authenticating completed student assessments.

13.2 Assessments are designed to require competency to be demonstrated through practical application, workplace/simulated workplace performance, observation, oral questioning, real artefacts and contextualised tasks where required by the training product.

13.3 Assessments shall avoid responding to generic written questions as the sole evidence for competence where AI could produce plausible answers without demonstrating the student's actual capability to apply in the workplace.

13.4 Students will be required to sign a declaration for every assessment submission and an AI acknowledgement for Green and Blue tasks.

13.5 Trainers may require additional evidence where authenticity is uncertain, including oral questioning, live demonstration, reflective explanation, version history, drafts, calculations, source notes or reassessment.

13.6 Group assessment tasks will require trainers to be able to identify individual student contribution and performance. Group work must not obscure whether each student is competent.

13.7 Trainers shall identify risk indicators such as sudden change in language level from student, unverifiable references, irrelevant generic content, inconsistent explanation, fabricated workplace details, missing process evidence or inability to demonstrate claimed work.

13.8 Academic-integrity concerns are reported to the RTO Manager.

14.0 Privacy, Confidentiality and Copyright

Area	Control
Personal and sensitive information	The Institute does not permit the entering of personal, sensitive, student, health, disability, financial, complaint, conduct, visa, USI, placement, employer/client or workplace information into public AI tools.
Privacy notices and consent	Where an approved AI tool handles personal information, update privacy notices and obtain consent where required. AI chatbots or student-facing tools must be clearly identified as AI-assisted.
Privacy Impact Assessment	The RTO Manager shall review instances where AI involves student records, profiling, automated decision support, proctoring, biometrics, vulnerable cohorts, support triage or substantial impact on a student. The RTO Manager shall provide reports of any issues or concerns at Management Team meetings.

Copyright and licensing	The Institute shall not permit the upload of commercial training resources, textbooks, third-party assessments, student submissions, images, videos or copyrighted materials to AI tools unless the licence allow it.
Indigenous cultural and sensitive content	The Institute shall not use AI to imitate First Nations cultural works, sacred/sensitive knowledge or community material. Use authentic consultation and permissions for cultural content.
Cybersecurity and accounts	All Institute personnel and students shall use Institute-approved accounts where available and appropriate. Users shall be advised to enable multifactor authentication for approved tools where available. Suspected data leakage or unauthorised AI use shall be reported to the RTO Manager immediately.
AI meeting notes and transcripts	AI note-taking requires prior notice and consent where appropriate. Transcripts or summaries must be human-reviewed before reliance, stored according to recordkeeping rules and not used for disciplinary, complaint or assessment matters without verification.

15.0 Responding to Suspected Misuse of AI

15.1 Suspected AI misuse is managed under the Academic Integrity Policy and Complaints and Appeals Policy. The purpose is to protect qualification integrity while applying procedural fairness. AI detection results, similarity scores, stylistic impressions or automated alerts are not enough by themselves to establish misconduct.

Procedure

15.2 The trainer identifies and records the concern, including the assessment task, relevant instructions, student declaration, evidence and reason the concern arose.

15.3 The trainer seeks clarification from the student and may resolve any minor issue or concern.

15.4 Should the trainer not be able to resolve the issue or concern, or the issue or concern is significant, the trainer reports the incident, in writing, to the RTO Manager. The RTO Manager conducts an initial review and decides whether more evidence is needed before judgement.

15.5 Student is given an opportunity to respond, explain how the work was produced and provide drafts, notes, version history or other process evidence.

15.6 If appropriate, the trainer may conduct oral questioning, practical demonstration, authenticity interview or supervised reassessment.

15.7 The RTO Manager, in consultation with the trainer, determines the outcome based on all evidence and records the rationale. Possible outcomes include no issue, additional evidence required, resubmission, reassessment, academic misconduct process, support intervention or disciplinary action.

15.8 Student is advised of the outcome and appeal rights.

15.9 The RTO Manager reports all significant incidents at the next Management Team meeting immediately following the incident.

16.0 Records and Evidence Retention

16.1 The Institute will maintain records sufficient to demonstrate compliance, self-assurance and continuous improvement.

16.2 Records and evidence may include:

- a) AI Tool Register and AI Use Case Register.
- b) AI risk assessments, privacy assessments, supplier due diligence and approvals.
- c) Student AI induction completions, declarations and AI acknowledgements.
- d) Trainer AI PD records, trainer AI use logs, resource review records and approvals.
- e) Assessment tool reviews showing AI category, authenticity controls and privacy warnings.
- f) Validation and moderation records that consider AI risks.
- g) Academic-integrity case files, authenticity interview records, reassessment records and appeal outcomes.
- h) Continuous improvement register entries arising from AI incidents, audits, student/trainer feedback or regulator updates.

17.0 Implementation Plan

Phase	Action	Owner	Target timeframe
Phase 1 - Governance setup	Appoint RTO Manager; approve policy; create AI Tool and Use Case Register, student declaration template and trainer AI log; update privacy/copyright warnings.	CEO / RTO Manager	Within 30 days of approval
Phase 2 - Student and trainer communication	Update Student Handbook, Trainer Handbook, assessment cover sheets, LMS announcements and induction modules. Publish plain-English student AI rules.	Training Manager / Student Support	Within 45 days
Phase 3 - Assessment uplift	Apply Red/Amber/Green/Blue AI categories to all current assessment tasks. Review AI-vulnerable tasks and implement authenticity controls.	Training Manager / Trainers / Assessors	Within 90 days
Phase 4 - Staff capability	Complete mandatory AI PD for trainers, assessors, support staff and administration. Include privacy, assessment integrity, source checking and incident escalation.	RTO Manager	Within 90 days and annually
Phase 5 - Validation and audit	Include AI controls in validation plan, internal audits and management review. Audit samples of student declarations, trainer logs and assessment instructions.	RTO Manager / Validation Panel	At next scheduled validation and quarterly quality review
Phase 6 - Review and improvement	Review AI incidents, student questions, appeals, regulator updates, vendor changes and assessment outcomes. Update policy and controls.	CEO / RTO Manager	At least annually or sooner if risk changes

18.0 Appendix A - Student AI Acknowledgement Template

Students complete this table when an assessment task is Green or Blue, or when the assessor requests AI use evidence.

Field	Student response
AI tool used	Example: ChatGPT, Microsoft Copilot, Grammarly, Gemini, Claude, translation tool or other approved tool.
Date(s) used	
Assessment task and unit	
Purpose of use	Example: brainstormed ideas, checked grammar, drafted structure, generated practice questions, compared options, summarised public material.
Prompt or instruction summary	I have not included any personal, sensitive, employer/client or confidential information.
AI output relied on	Briefly explain what was used and what was discarded.
How I checked the output	List sources, trainer notes, legislation, training materials, industry references, calculations or practical checks.
Changes I made	Explain how you edited, corrected, contextualised or applied the AI output.
Student declaration	I declare that the final assessment evidence is my own work and that I can explain and demonstrate the knowledge and skills submitted. Student Name: _____ Student Signature: _____ Date: _____

19.0 Appendix B - Trainer AI Use Log

Field	Trainer entry
Date	
Trainer/assessor	
Tool used	
Purpose	Lesson plan / formative activity / resource draft / assessment draft / feedback template / policy draft / other.
Prompt summary	Do not record personal, student, workplace or confidential information.
Output used	Brief description of content retained or adapted.
Verification completed	Training product checked / TAS checked / legislation checked / industry source checked / copyright checked / LLN/accessibility checked.
Approval required?	Yes / No. If yes, record approver and date.
Final storage location	Email completed AI Log to the RTO Manager prior to conducting assessment.
Trainer declaration	I declare that the assessment practice complies with the Principles of Assessment and Rules of Evidence. Trainer Name: _____ Trainer Signature: _____ Date: _____

20.0 Appendix C - AI Tool Register and AI Use Case Register

Risk area	Review		
Context for use of AI	Training delivery / Assessment / Admin / Other	Date	
Purpose and necessity	Is AI necessary and proportionate? What problem does it solve? Is there a lower-risk non-AI method?		
Data types	Will the tool handle personal, sensitive, student, assessment, workplace, commercial, health, disability, financial, biometric or copyrighted information?		
Assessment impact	Could the AI affect assessment instructions, evidence collection, judgement, feedback, results, RPL, credit, certification or academic-integrity allegations?		
Student impact	Could the tool affect access, inclusion, disability adjustments, support, progression, complaints, appeals or disciplinary action?		
Privacy and security	Where is data stored? Who can access it? Is data used for model training? What retention/deletion controls exist? Is MFA available? What breach notification applies?		
Transparency	Will students or staff know AI is being used? Are privacy notices, assessment instructions and user warnings updated?		
Bias and accuracy	How will outputs be checked? What data quality or bias risks exist? What human review is required?		
Contestability	Can a student challenge the AI-supported process or outcome? Can the RTO explain the role of AI and provide a human review?		
Supplier and contract	Are terms of service, privacy policy, security controls, data ownership, IP rights, auditability and subcontractors acceptable?		
Records and review	What records will be kept? Who owns the use case? When will it be reviewed? What incidents must be reported?		
RTO Manager declaration	I declare that the use of AI complies with the St Peter Institute's AI Policy Name: _____ Signature: _____ Date: _____		