

Transport Professionals Association Artificial Intelligence (AI) Usage Policy

DOCUMENT AND DATA CONTROL | PD-027

Distribution Controlled

This means:

1. Distribution is centralised - in this case from the Board of Directors.
2. Each copy is issued to a particular person or organisation. If no longer required, it should be returned.
3. It is not to be photocopied either in whole or in part and unless this page is over-stamped with the words "UNCONTROLLED COPY", Additional copies are available on request.
4. Controlled copy holders will be automatically issued with any amendments. Responsibility for incorporating such amendments rests with the copy holder.
5. This document is not to be distributed outside Transport Professionals Association (formerly AITPM) unless approval is given by the Board of Directors. Clients may peruse this document at the discretion of the Board ie (for audit purposes).
6. External issues of this document issued strictly "Commercial in Confidence".

REVISION STATUS								
Rev No	Date	Revision Description	Intl	Sign	Intl	Sign	Intl	Sign
			Prepared		Checked		Approved	
V1	27/07/2026	Policy creation	KK		Board		Board	

Transport Professionals Association Artificial Intelligence (AI) Usage Policy

1. Purpose

The purpose of this policy is to enable the safe, responsible and productive use of Artificial Intelligence (AI) by TPA while protecting TPA's information, people, members, partners, reputation and governance obligations.

TPA recognises that AI can improve productivity, support research, strengthen drafting and analysis, enhance accessibility, and help staff manage complex workloads. AI must, however, be used with professional judgement, human accountability, transparency and appropriate security controls.

2. Scope

This policy applies to all TPA employees, contractors, consultants, volunteers, Board members, and any other authorised person using AI tools for TPA work or on TPA's behalf.

The policy applies to all AI-enabled systems used for work, including standalone generative AI platforms, enterprise AI services, AI features embedded in software, automated transcription or note-taking tools, AI search tools, image or video generation tools, translation tools, writing assistants and AI-enabled workflow or project management tools.

3. Guiding Principles

Principle	What it means for TPA
Human accountability	A person remains responsible for all decisions, advice, communications, approvals and work products. AI must not be treated as an authority or decision-maker.
Security and privacy by design	TPA information must only be used in approved environments and in accordance with privacy, confidentiality, records and cyber security obligations.
Accuracy and evidence	AI outputs must be checked for accuracy, source quality, currency, completeness and relevance before use.
Transparency	AI use should be disclosed where it materially contributes to significant, public-facing, governance, policy, advocacy or member-facing work.
Fairness and ethics	AI must not be used to generate discriminatory, misleading, harmful, deceptive, exploitative or inappropriate content.
Proportionate governance	The level of review and approval must reflect the risk, audience, sensitivity and potential impact of the work.

4. Definitions

Term	Meaning
AI	Software or systems that can generate, summarise, classify, predict, recommend, analyse, automate or transform content, data or decisions using machine learning, generative AI or related techniques.

Term	Meaning
Generative AI	AI that creates or transforms content, including text, images, code, audio, video, presentations, summaries or analysis.
Approved enterprise AI	AI tools approved by TPA for work use and accessed through an organisational account, with appropriate contractual, security, privacy and administrative controls.
Public AI tool	A generally available AI service that is not controlled by TPA and may have different data retention, privacy, model training, confidentiality or security settings.
Confidential information	Non-public TPA information including Board papers, minutes, member data, staff information, financial information, legal advice, commercial information, passwords, contracts and partner data.

5. AI Tool Categories

TPA will maintain an Approved AI Tools Register (See Initial Register at Appendix A). The register may be updated by the CEO or delegate as tools, licences, contractual terms, security controls and organisational needs change.

Category	Examples	Permitted use	Conditions
Approved enterprise AI	Microsoft 365 Copilot, Copilot Chat with TPA work account, Copilot in Word, PowerPoint, Excel, Outlook and Teams.	General work use including drafting, summarising, meeting support, analysis, document preparation and productivity support.	Use only through TPA work accounts; comply with permissions, retention, labels, records and review requirements.
Conditionally approved embedded AI	Xero, Asana AI, Canva AI, Tango, ApprovalMax, Weel, EventsAir, Adobe Firefly or Adobe AI features, Grammarly or writing assistants, other business software AI features.	May be used where approved for the task and no confidential, sensitive or personal information is entered unless the tool is approved for that data type.	Check the Approved AI Tools Register. Use only within approved accounts, settings and data boundaries.
Public AI tools requiring caution	Public versions of ChatGPT, Claude, Gemini, Perplexity, consumer image generators, browser AI assistants and similar tools.	May be used for low-risk, non-confidential ideation, generic drafting, brainstorming or learning.	Do not enter confidential, personal, member, Board, financial, legal, HR, partner, contract or unpublished TPA information. Outputs require verification.
Prohibited or high-risk use	Any AI tool used to process restricted data without approval; tools that require unauthorised data upload; AI used for automated decisions about people.	Not permitted unless specifically approved by the CEO and, where required, the Board or legal/privacy advisers.	Includes attempts to bypass security controls, generate misleading material, impersonate people or produce inappropriate or discriminatory content.

6. Approved and Acceptable Uses

Subject to this policy, AI may be used to support:

- Drafting, editing, summarising and restructuring documents, emails, reports, presentations and meeting notes.
- Preparing first drafts of internal material, project plans, content calendars, task lists and briefing notes.

- Summarising meetings, chats, files and emails where the user has authorised access and the tool is approved for that information.
- Analysing non-sensitive data, identifying themes, preparing options, creating scenarios and supporting decision preparation.
- Developing learning resources, CPD outlines, event programs, marketing concepts and communication drafts.
- Improving accessibility, readability, plain language, translation and formatting where the output is checked by a human.
- Creating low-risk design concepts, graphics or social media draft assets where copyright, attribution and brand requirements are checked.

7. Prohibited Uses

AI must not be used to:

- Upload, disclose or process confidential, personal, Board, legal, HR, financial, partner, contract or member information in unapproved AI tools.
- Make automated decisions about employment, membership, discipline, complaints, awards, grants, procurement or access to opportunities without human review and approved process controls.
- Generate or publish false, misleading, deceptive, defamatory, discriminatory, harassing, unlawful, unsafe or inappropriate content.
- Circumvent TPA security settings, passwords, access controls, records management requirements or approval processes.
- Impersonate a person, fabricate quotes, create fake endorsements, misrepresent TPA's position or obscure accountability for work.
- Use AI-generated legal, financial, governance, employment, technical or professional advice as final advice without appropriate expert review.
- Record, transcribe or summarise meetings without appropriate notice, consent or compliance with TPA meeting practices and applicable law.

8. Data Protection and Privacy

Users must protect TPA information according to its sensitivity. The following handling rules apply:

Information type	Examples	AI handling rule
Public	Published website content, public event information, public submissions.	May be used in approved or public AI tools, subject to accuracy, attribution and copyright review.
Internal	Routine internal planning, non-sensitive operational notes, draft task lists.	May be used in approved enterprise AI. Use caution in public AI tools and remove identifying context where possible.
Confidential	Board papers, financial reports, member lists, staff matters, contracts, sponsorship details, legal advice, unpublished policy positions.	Use only in approved enterprise AI where the user has authorised access and the tool is approved for that data. Do not use in public AI tools.
Restricted or sensitive	Passwords, credentials, health information, sensitive personal information, complaints, disciplinary matters, sensitive HR information.	Do not use in AI tools unless specifically approved by the CEO and supported by appropriate legal, privacy and security controls.

Personal information must be handled in accordance with TPA's privacy obligations and the Australian Privacy Principles. Users must minimise personal information in prompts and outputs and must not enter personal information into any public AI tool unless specifically authorised and legally appropriate.

9. Microsoft 365 Copilot Use

Microsoft 365 Copilot and Microsoft 365 Copilot Chat may be used as approved enterprise AI tools when accessed through a TPA work account and configured within TPA's Microsoft 365 environment.

When using Microsoft 365 Copilot, users must:

- Only use the TPA work account, not a personal Microsoft account, for TPA work.
- Understand that Copilot can only use content the user is already authorised to access, which means good permissions hygiene remains essential.
- Avoid asking Copilot to retrieve, summarise or expose material that the user does not have a legitimate business need to use.
- Review meeting summaries, document drafts, email drafts, data analysis and citations before sharing or relying on them.
- Treat Copilot outputs as drafts or assistance, not final advice, official records or approved organisational positions.
- Ensure Board, HR, finance, legal, member and partner information remains governed by TPA's permissions, storage, retention and approval requirements.

Before expanding Microsoft 365 Copilot use, TPA should maintain effective SharePoint, OneDrive, Teams and Exchange permissions, sharing controls, sensitivity labels, retention settings, audit capability and staff guidance.

10. AI in Meetings, Transcription and Notes

AI meeting summary, transcription and note-taking tools may only be used where the meeting organiser is authorised to do so and participants are appropriately informed. For Board, HR, complaints, legal, finance or confidential partner meetings, AI transcription or summarisation must not be enabled unless approved by the CEO, Company Secretary or meeting chair and consistent with records and confidentiality requirements.

11. Accuracy, Verification and Human Review

All AI-generated work must be reviewed by a human before it is relied upon, shared or implemented. The reviewer must check accuracy, completeness, tone, source quality, currency, privacy, copyright, legal risk, member impact and alignment with TPA's position.

Work type	Minimum review requirement
Routine internal drafts, notes, task lists and administrative material	User review before use.
Member emails, newsletter text, event promotions and routine public communications	Manager or CEO review according to normal communications approvals.
Board papers, Council papers, governance documents and policies	CEO review before circulation; Board approval where required.
Submissions, advocacy, technical advice, position statements and media material	CEO review and additional subject matter review where appropriate.
Finance, HR, legal, disciplinary, complaints or sensitive member matters	CEO review and external professional advice where appropriate.
External images, graphics, video or brand assets	Brand, copyright and appropriateness review before publication.

12. Transparency and Attribution

AI use should be disclosed where it materially contributes to significant governance, policy, advocacy, technical, member-facing or public-facing work. Disclosure does not need to be made for routine spelling, grammar, formatting, brainstorming or minor drafting support unless a specific stakeholder, funder, publication or legal requirement applies.

Where AI-generated images, designs, data visualisations or creative assets are used externally, staff must check copyright, licensing, permissions, attribution requirements and brand suitability before publication. This includes obtaining confirmation from third parties such as volunteers and partners who provide this content.

13. Intellectual Property and Copyright

Work created by staff, contractors or authorised representatives for TPA, including AI-assisted work, remains TPA work product unless otherwise agreed in writing. Users must not upload third-party copyrighted material into AI tools unless permitted by licence, law or agreement, and must not publish AI-generated output that appears to reproduce protected material without review.

14. Roles and Responsibilities

Role	Responsibilities
Board	Approve the policy and set risk appetite for organisational AI use.
CEO	Own the policy, approve the Approved AI Tools Register, oversee implementation, approve exceptions and report material risks to the Board.
Managers / project leads	Ensure staff use AI appropriately, review higher-risk outputs and identify training or compliance issues.
Users	Use AI responsibly, protect information, verify outputs, disclose use where required and report incidents promptly.
IT support provider	Assist with Microsoft 365 configuration, permissions, security, audit, retention and tool assessment as requested.

15. Training and Awareness

Users authorised to use AI for TPA work must complete responsible AI training or briefing approved by the CEO. Training should cover tool categories, data protection, privacy, prompt safety, hallucination and accuracy risks, copyright, transparency, Microsoft 365 Copilot use and incident reporting.

16. Incidents and Concerns

Users must promptly report any suspected AI-related data exposure, privacy incident, copyright issue, misleading output, inappropriate content, security concern or breach of this policy to the CEO. The CEO will determine whether further investigation, notification, containment, legal advice, IT action or Board reporting is required.

17. Monitoring, Records and Assurance

TPA may monitor AI use where lawful and appropriate to protect information, meet compliance obligations, investigate incidents, improve training and ensure responsible use. AI-generated work that forms part of TPA's official records must be saved and managed in TPA's approved records or document management locations.

18. Breaches

Breaches of this policy may result in corrective action, removal of access, retraining, disciplinary action, contract action or other consequences appropriate to the nature and seriousness of the breach.

19. Review

This policy will be reviewed by 30 June 2027, or earlier if there is a material change in law, technology, Microsoft 365 Copilot configuration, TPA systems, information security risk, privacy requirements or Board risk appetite.

Appendix A – Initial Approved AI Tools Register

Tool / category	Initial status	Permitted TPA use	Key controls
Microsoft 365 Copilot and Copilot Chat with TPA work account	Approved enterprise AI	Drafting, summarising, meeting assistance, email and document support, analysis of accessible work content.	Use TPA account only; observe permissions, labels, retention, confidential information rules and review requirements.
Copilot in Teams meetings	Approved with conditions	Meeting recap, summaries and action support for appropriate meetings.	Inform participants; do not use for sensitive meetings unless approved by CEO or chair.
Asana AI	Conditionally approved	Project summaries, task support, workflow assistance and status reporting.	Do not include confidential or sensitive data unless approved for that data type.
Xero AI features	Conditionally approved	Finance workflow support, coding suggestions, report assistance and administrative productivity where available.	Use only through approved TPA account settings; review outputs carefully; do not rely on AI-generated financial treatment without human verification.
Tango	Conditionally approved	Process documentation, workflow capture, step-by-step guides and internal training materials.	Check screenshots and captured content for confidential, personal, member, financial or system access information before sharing or publishing.
ApprovalMax	Conditionally approved	Finance workflow, approval routing, expenditure controls and reporting support where AI or automation features are available.	Use only through approved TPA account settings; maintain delegated authorities and human approval; verify any suggested coding, routing or approval information.
Weel	Conditionally approved	Expense management, receipt processing, spend visibility, card administration and finance workflow support where AI or automation features are available.	Use only through approved TPA account settings; verify expense coding and receipt extraction; do not rely on automated classification without finance review.
EventsAir	Conditionally approved	Event administration, registration workflows, attendee communications, reporting and event delivery support where AI or automation features are available.	Use only through approved TPA account settings; protect attendee, member, sponsor and payment information; review automated

Tool / category	Initial status	Permitted TPA use	Key controls
			communications and reports before use.
BoardPro	Conditionally approved	Board and committee administration, meeting pack preparation, agenda management, minutes support, action tracking and governance workflow support where AI or automation features are available.	Use only through approved TPA account settings; protect Board, committee, financial, strategic and confidential information; review AI-assisted minutes, summaries and actions before circulation or approval.
Adobe Firefly / Adobe AI features	Conditionally approved	Image editing, creative concept development and design assistance.	Check licensing, attribution, brand and publication approvals.
Public generative AI tools	Limited use only	Generic brainstorming, low-risk drafting, learning and non-confidential research prompts.	No confidential, personal, Board, member, staff, partner, contractual, legal or financial information.
Unapproved meeting transcription bots or browser extensions	Not approved unless assessed	Not to be used for TPA meetings unless approved.	CEO approval required; privacy, consent, storage and access settings must be reviewed.

Appendix B – Quick Prompt Safety Guide

Prompt type	Allowed?	Example
Generic brainstorming with no confidential content	Yes	Give me five structure options for a governance policy on responsible AI use.
Summarising a draft stored in TPA Microsoft 365 that you are authorised to access	Yes, in Microsoft 365 Copilot	Summarise the key decisions requested in this Board paper and identify any unclear recommendations.
Uploading a member list into a public AI tool	No	Not permitted. Use approved systems only and only where there is a legitimate business need.
Asking AI to write a final public position statement without review	No	AI may help draft, but CEO and subject matter review are required before publication.
Using AI to make a disciplinary or membership eligibility decision	No automated decision	AI may help organise information if approved; a human decision-maker must apply the approved process.

Key Contacts

Kirsty Kelly
CEO
Transport Professionals Association
+61 7 3544 5670
kirsty.kelly@transportprofessionals.com.au