Artificial Intelligence & Technology Use Policy

Business: MarketingSteve
ABN: 52719351544
Effective Date: October-2026
Last Reviewed: October-2026
Review Frequency: Annually or following material technological or regulatory changes

1. Purpose

This policy establishes the standards governing the responsible use of artificial intelligence (AI), automation and related digital technologies by MarketingSteve.

The objective is to support innovation, efficiency and high-quality professional services while protecting client confidentiality, information security, intellectual property and professional integrity.

AI and other digital technologies are intended to support, rather than replace, professional expertise and judgment.

All work delivered to clients must reflect meaningful professional involvement, appropriate verification and the standards expected of a qualified marketing consultant.

2. Scope

This policy applies to the use of AI-assisted technologies and digital tools in connection with:

- Marketing research and analysis.
- Strategic planning and advisory services.
- Copywriting, content creation and communications.
- Brand development and creative activities.
- Marketing performance analysis and reporting.
- Administrative and operational activities.
- Automation and workflow management.
- Client service delivery and related professional work.

This policy applies to the sole trader and any subcontractors or freelancers authorised to undertake work on behalf of the business.

3. Permitted Use of AI

AI-assisted tools may be used where their application is appropriate to the task, consistent with the client's requirements and compatible with the business's professional obligations.

Permitted uses may include:

- Exploring ideas, concepts and alternative approaches.
- Supporting research and identifying information for further investigation.
- Assisting with strategic analysis and planning.
- Preparing preliminary content and copywriting drafts.
- Organising, summarising and structuring non-restricted information.
- Supporting analysis of appropriately authorised and minimised data.
- Improving administrative efficiency and internal workflows.
- Assisting with quality assurance and document review.

The use of AI must be proportionate to the nature of the work and must not compromise its accuracy, originality, confidentiality or professional quality.

AI tools must not be used simply because they are available where their use would introduce unnecessary risk or reduce the quality of the Services.

4. Professional Responsibility and Human Oversight

The consultant retains professional responsibility for work undertaken with the assistance of AI.

AI-generated outputs must be treated as preliminary material requiring appropriate professional assessment.

Before incorporating AI-assisted material into client deliverables, the consultant must:

- Review its accuracy, relevance and suitability.
- Apply independent professional judgment.
- Verify material factual claims, statistics and references where appropriate.
- Consider potential limitations, assumptions or bias.
- Ensure the work addresses the client's actual objectives and circumstances.
- Make substantive revisions or additions where necessary to meet the required professional standard.

AI-generated recommendations must not be accepted without appropriate consideration of their commercial rationale and supporting evidence.

The consultant must remain capable of explaining the professional basis for significant recommendations, regardless of whether AI assisted their development.

5. Prohibition on Raw AI Deliverables

Raw AI-generated outputs must never be presented to clients as completed professional deliverables.

All AI-assisted deliverables must demonstrate meaningful professional involvement, including appropriate review, interpretation, development, refinement or application of specialist knowledge.

Minor cosmetic editing alone does not constitute adequate professional review where substantive assessment is required.

The consultant must not represent AI-generated material as independently researched, verified or professionally developed where that representation would be misleading.

AI may accelerate the development of work, but it must not substitute for the professional value and accountability expected from the consultant.

6. Accuracy and Verification

AI systems may generate inaccurate information, fabricated references, incomplete analysis or misleading conclusions.

Information produced or suggested by AI must be treated according to its reliability and the significance of the intended use.

Where relevant, the consultant must:

- Verify important factual statements against reliable sources.
- Confirm that cited publications, statistics and references exist and support the relevant claims.
- Review calculations and interpretations of data.
- Distinguish factual findings from assumptions or predictions.
- Identify material limitations in AI-assisted research.
- Avoid reliance on unsupported conclusions.

The level of verification required must be proportionate to the significance and potential consequences of the work.

AI-generated information must not be presented as verified evidence unless appropriate verification has occurred.

7. Confidentiality and Client Information

The consultant must protect confidential information and personal information in accordance with the Privacy Policy, Information Security & Client Data Handling Policy and applicable client agreements.

Identifiable personal information, sensitive information and materially confidential client information must not be intentionally submitted to external generative AI systems unless:

(a) the Client has expressly authorised the relevant use in writing;

(b) the proposed use is reasonably necessary and appropriate for the Services;

(c) the relevant tool's security, retention and information-handling arrangements have been reasonably assessed; and

(d) applicable privacy, confidentiality and other legal obligations can be satisfied.

Client authorisation does not, by itself, override legal restrictions on the disclosure or processing of personal information.

Where practicable, the consultant must use anonymised, aggregated, de-identified or otherwise minimised information instead of identifiable or confidential source material.

The consultant must not upload entire client databases, sensitive records, confidential commercial documents or substantial amounts of restricted information merely for convenience.

8. Client-Owned Platforms and Data Storage

Where reasonably practicable, client information should remain within client-owned or client-controlled systems.

The consultant may use business-controlled devices, accounts and cloud services for legitimate working documents and other information reasonably necessary for service delivery, subject to appropriate security arrangements.

AI tools must not be given unnecessary access to client systems, databases or cloud storage.

Connections between AI services and client-owned platforms must only be established where appropriately authorised and reasonably necessary for the agreed work.

The consultant must consider the information accessible through any connected tool, not only the information intentionally included in a particular prompt.

9. Selection and Security of AI Tools

AI and other digital tools used for business purposes should be selected with reasonable regard to their intended function, reliability, security and information-handling practices.

Before adopting a tool for material client work, the consultant should consider, where relevant:

- The tool's purpose and suitability.
- Its reliability and known limitations.
- The nature of information it collects or processes.
- Whether information may be retained or used for model training.
- Whether information may be disclosed to additional service providers.
- Relevant data storage and processing locations.
- Available privacy and security controls.
- Access permissions and authentication requirements.
- Applicable subscription and licensing terms.

Where practical and appropriate, settings that unnecessarily permit confidential business information to be used for third-party model training or unrelated purposes should be disabled.

Tools presenting an unacceptable security, confidentiality or legal risk must not be used for the affected activities.

10. Intellectual Property and Originality

AI-assisted work must be developed with reasonable regard to applicable copyright, licensing and intellectual property requirements.

The consultant must not knowingly use AI tools to reproduce protected third-party material without appropriate authorisation.

Where AI-generated materials are incorporated into deliverables, reasonable consideration must be given to originality, potential infringement and any relevant licensing restrictions.

The consultant must not assume that AI-generated content is automatically eligible for copyright protection or that exclusive intellectual property ownership can always be transferred to a client.

Where intellectual property rights or licensing arrangements are material to the proposed work, the consultant should clarify the relevant limitations and seek specialist advice where reasonably necessary.

Client-supplied intellectual property must only be used for authorised purposes.

11. AI-Generated Images, Audio and Video

AI-generated visual, audio and video content may be used where appropriate to the agreed work and applicable legal requirements.

However, the consultant must not knowingly create or distribute:

- Deceptive impersonations of real individuals.
- Fabricated testimonials or endorsements.
- Misleading representations of real events or products.
- Unauthorised reproductions of identifiable individuals where consent or other lawful authority is required.
- Material intended to deceive an audience about its authenticity.

Where the use of synthetic content may materially affect an audience's understanding, appropriate disclosure or contextual information should be considered.

12. Regulated Industries and High-Risk Activities

Additional care must be exercised when using AI in connection with regulated industries, including financial services, healthcare and other sectors subject to specific marketing or communication requirements.

AI-assisted content involving regulated claims, products or services must be appropriately reviewed before publication or implementation.

Where reasonably necessary, relevant materials should be referred to the client's authorised legal or compliance personnel.

AI must not be relied upon as a substitute for specialist legal, financial product, regulatory or other professional advice.

The consultant must not use AI to make consequential decisions about identifiable individuals, including decisions affecting their eligibility, rights or access to services, without expressly agreed authority, appropriate safeguards and consideration of applicable law.

13. Automation and Digital Workflows

Automation may be used to improve efficiency and support routine business or marketing activities.

Where an automated process can publish content, send communications, modify client records, incur expenditure or take other material actions, appropriate controls must be established.

These may include:

- Clearly defined permissions and operational limits.
- Client approval where required.
- Testing before implementation.
- Human review of higher-risk actions.
- Monitoring for errors or unintended activity.
- The ability to pause or disable the process where reasonably practicable.

Automation must not exceed the consultant's delegated authority.

The consultant must not knowingly implement automated activities that breach applicable marketing, privacy or consumer protection requirements.

14. Client Transparency and Disclosure

The consultant may use AI-assisted technologies as part of normal professional workflows where permitted by the relevant agreement and this policy.

The consultant is not ordinarily required to disclose every incidental use of AI for research, drafting, organisation or administrative assistance.

However, the consultant must:

- Comply with any AI disclosure requirements agreed with the Client.
- Be truthful when directly asked about the use of AI.
- Disclose material AI involvement where necessary to avoid misleading the Client.
- Obtain appropriate authorisation before restricted client information is processed through external AI services.
- Identify significant AI-related limitations where they may materially affect the Client's decisions.

The use of AI must not be concealed where doing so would be misleading or inconsistent with a contractual or legal obligation.

15. Third-Party Providers and Subcontractors

Where subcontractors or freelancers use AI or other digital tools in connection with work undertaken for the business, they must observe appropriate confidentiality, information security and professional standards.

Subcontractors must not submit restricted client information to external AI services without the necessary authorisation.

Work produced with AI assistance remains subject to appropriate professional review before delivery to the Client.

The consultant must exercise reasonable care when engaging and supervising subcontractors, having regard to the scope and nature of the work.

16. Technology Incidents and Errors

Suspected unauthorised disclosure of client information, compromised tool access, significant automation failures or other material technology incidents must be addressed promptly.

Where personal or confidential information may have been compromised, the Data Breach & Incident Response Procedure must be followed.

Where AI-assisted work is found to contain a material error, the consultant must assess the potential impact and take reasonable corrective action.

This may include revising affected work, notifying the Client where appropriate, suspending an automated process or reviewing the relevant tool's suitability.

17. Professional Development and Review

The consultant will take reasonable steps to remain informed about developments in AI and other technologies relevant to the Services.

This includes awareness of material changes to tool capabilities, privacy and security risks, professional expectations and applicable legal requirements.

The adoption of new technologies should be guided by their practical value, suitability and risk rather than novelty alone.

18. Policy Review

This policy will be reviewed at least annually and following material changes to the business's technology use, services, legal obligations or identified risks.

The consultant is responsible for ensuring the policy remains appropriate to the business's size, operations and professional responsibilities.