POLICY DOCUMENT

Artificial Intelligence

Acceptable Use Policy

Organisation: [Organisation Name]
Version: 1.0
Effective Date: [Date]
Review Date: [Date + 12 months]
Policy Owner: [Name / Role]

Prepared by [IT Provider Name]

1. Purpose

This policy establishes the acceptable use of artificial intelligence tools within [Organisation Name]. It applies to all staff, contractors, volunteers, and any person acting on behalf of the organisation who uses artificial intelligence tools in connection with their work.

Artificial intelligence tools offer real productivity benefits. The purpose of this policy is not to prohibit their use, but to ensure they are used in a way that protects the organisation, its clients, and the personal information it holds.

WHY THIS POLICY EXISTS

Free and consumer-grade artificial intelligence tools are not designed for business use. Data submitted to these tools may be retained by the provider, used to train future models, reviewed by human operators, or processed in data centres outside New Zealand. This creates privacy, confidentiality, and legal risk that organisations have an obligation to manage.

---

2. Scope

This policy applies to all permanent and fixed-term employees, contractors, consultants, temporary staff, volunteers, and any third party acting on behalf of the organisation, on any device used for work purposes.

---

3. Definitions

Term	Definition
AI Tool	Any software using machine learning or large language models to generate or process content. Examples include Microsoft Copilot, ChatGPT, Claude, and Google Gemini.
Free-Tier Account	An account not covered by a business or enterprise agreement. Data may be retained and used to train future models.
Enterprise Account	A business or enterprise agreement including data processing commitments and zero data retention.
Personal Information	Any information about an identifiable individual, as defined under the Privacy Act 2020.
Prompt	The text or other input a user submits to an AI tool to generate a response.
Hallucination	A factually incorrect or fabricated response produced by an AI tool, presented with apparent confidence.

---

4. Legal and Regulatory Framework

Privacy Act 2020

Requires organisations to protect personal information against loss, misuse, and unauthorised access. Submitting personal information to a consumer AI tool may not be consistent with this obligation. Notifiable breaches must be reported to the Office of the Privacy Commissioner as soon as practicable.

Health Information Privacy Code 2020

Health information must never be submitted to any AI tool unless covered by a signed data processing agreement satisfying the Code's requirements.

Employment Relations Act 2000

Staff use of AI tools must be consistent with employment obligations including the duty of good faith and any confidentiality clauses.

Harmful Digital Communications Act 2015

AI tools must not be used to create or distribute content that is harmful, threatening, or harassing.

---

5. Approved and Prohibited Tools

5.1 Approved Tools

Tool	Approved Plan	Conditions
Microsoft Copilot	Microsoft 365 licensed tenant only	Do not use consumer copilot.microsoft.com
[Tool Name]	[Plan type]	[Conditions]

5.2 Prohibited Tools

- Consumer or free-tier accounts on any AI platform not listed above
- AI tools with data residency in jurisdictions without adequate privacy protections, including DeepSeek
- AI tools without a published privacy policy or data processing terms

---

6. Data Classification

Classification	Examples	AI Use Permitted?
Public	Marketing content, published reports	Yes — approved tools only
Internal	Internal procedures, non-sensitive meeting notes	Yes — remove names and identifying details first
Confidential	Client personal information, financial records, contracts, credentials	**No — prohibited without written approval from [Policy Owner]**
Restricted	Health records, identity documents, passwords, payment card data	**Never — absolutely prohibited**

---

7. Acceptable Use

- Only use AI tools listed in the approved tools table
- Only use work or organisational accounts — never personal accounts for work tasks
- Do not submit confidential or restricted information to any AI tool
- Always review AI-generated output before using it — never rely on it without verification
- Do not submit prompts on behalf of clients without their knowledge and consent
- Multi-factor authentication must be enabled on all AI accounts used for work
- Verify any factual claims, statistics, or citations independently before relying on them

---

8. Prohibited Use

- Submitting client personal information, health records, passwords, or identity documents
- Using consumer or free-tier AI accounts for work tasks
- Generating malicious code, phishing content, or content intended to cause harm
- Generating content that harasses, threatens, or discriminates against any individual or group
- Circumventing security controls, access restrictions, or organisational policies

PRIVACY ACT 2020 — REMINDER

Submitting personal information about clients or staff to a consumer AI tool likely constitutes disclosure to a third party without appropriate safeguards, and may constitute a notifiable privacy breach under the Privacy Act 2020.

9. Output Verification

AI tools can produce inaccurate, biased, or entirely fabricated output. Staff must read and assess all AI output, verify factual claims and citations independently, confirm no confidential information has been included, and have output reviewed before sending externally.

LEGAL AND PROFESSIONAL ADVICE

AI tools must never substitute for legal, financial, or medical advice. In 2023, New York attorneys were sanctioned for submitting AI-generated case citations that did not exist (Mata v. Avianca Inc., SDNY). Always verify AI output independently.

10. Incident Reporting

Report the following to [IT Manager / IT Provider] immediately:

- Accidental submission of confidential or personal information to an AI tool
- Suspected compromise of an AI account
- Discovery of AI tool use that appears to breach this policy

11. Breach of Policy

Breach of this policy may result in disciplinary action up to and including termination of employment. Where a breach results in a notifiable privacy breach under the Privacy Act 2020, the organisation must notify the Office of the Privacy Commissioner and affected individuals.

12. Staff Acknowledgement

I confirm that I have read, understood, and agree to comply with this Artificial Intelligence Acceptable Use Policy.

Full Name

Role

Signature

Date

Document Control

Version	Date	Author	Summary of Changes
1.0	[Date]	[IT Provider Name]	Initial version

Prepared by [IT Provider Name] | [IT Provider Website] | [IT Provider Phone]