



Artificial Intelligence (AI) Acceptable Use Policy

Purpose

This policy sets clear expectations for how Artificial Intelligence (AI) tools may be used in our workplace. AI can help us be more productive, creative, and efficient, but it must be used responsibly, securely, and ethically.

This policy ensures we protect people, data, intellectual property, and our reputation while complying with New Zealand legislation including the Privacy Act 2020, Human Rights Act 1993, Employment Relations Act 2000, and Copyright Act 1994. It also makes clear that AI supports but never replaces human judgment and accountability.

Scope

This policy applies to all employees, contractors, consultants, and third parties using AI tools on behalf of the company. It covers both company-built AI systems and external platforms such as ChatGPT, Microsoft Copilot, Claude, Adobe Firefly, and Google Gemini.

AI tools may only be used when approved by the company and with access provisioned through the company's secure IT processes.

As far as our expectations are concerned (as set out below), these expectations also apply to workplace participants that are not employees (for example, independent contractors and volunteers). Instead of disciplinary action, breaches of our requirements by those workplace participants may result in the termination of their contract or volunteer agreement (without the need for a disciplinary process).

Key Principles

Our approach to AI is built on the following principles:

Transparency

Employees must be open about when and how AI is used, particularly where others rely on the outcome.

Human Oversight and Accountability

AI may support work, but employees remain responsible for the accuracy, legality, and impact of all outputs.

Fairness and Non-Discrimination

AI use must be free from bias, discrimination, or harmful assumptions.

Privacy, Security, and Safety

AI use must comply with privacy law, cyber-security requirements, industry standards, and must avoid creating risks to employee wellbeing or workplace health and safety.

Employee Responsibilities

Employees must:

- Use AI only for business-related purposes and in line with company standards.
- Review and validate all AI outputs for accuracy, fairness, legality, copyright compliance, and suitability.
- Validate all facts, statistics, and figures generated by AI before using or distributing content.
- Disclose when AI has contributed significantly to documents, reports, designs, or communications used by others.
- Not enter confidential or personal information into AI tools unless approved for secure use.
- Ensure compliance with local and foreign privacy and data-handling laws where applicable.
- Ensure content is professional, respectful, and does not involve sensitive demographics in inappropriate contexts.
- Avoid placing information into systems that may be auto-ingested by AI without authorisation.

Manager Responsibilities

Managers must:

- Set expectations for when AI use should be disclosed.
- Ensure employees remain accountable for the quality of their work.
- Monitor AI use and provide guidance where needed.
- Ensure employee-sensitive or confidential client information is never input into AI tools unless authorised.
- Validate that data accessible to AI-enabled tools cannot be surfaced beyond permission groups.
- Ensure new employees complete any required AI and security training (if applicable).
- Ensure AI features within existing tools remain disabled until reviewed and approved.
- Prevent staff from using approved platforms to create insecure AI agents or automations.

Security and Data Protection

To protect information, the company requires that AI tools are used only when they have been formally approved, particularly when handling company or client data. Confidential, personal, or sensitive information must never be entered into public or unauthorised AI systems. Employees must comply with all company security practices, including using password managers, Single Sign-On (SSO), and Multi-Factor Authentication (MFA), and must report any AI-related phishing attempts or suspicious activity immediately. AI tools may only be accessed through IT-provisioned accounts, and their use on personal devices connected to company networks is prohibited unless specific authorisation is provided.

Intellectual Property and Attribution

All AI-generated content created during your employment is owned by the company. Employees must ensure AI tools are not used to replicate or imitate copyrighted materials, such as logos, imagery, or design styles, without the necessary permission. When AI-generated content is used externally, appropriate disclosure must be made in line with company standards and legal requirements. Employees must also review all AI-generated outputs, particularly images, audio, and video, to assess potential copyright risks or intellectual property conflicts before use or publication.

Acceptable Use

AI must only be used for lawful, ethical, and business-related purposes. Employees must:

- Avoid offensive, discriminatory, or harmful content.
- Obtain consent before generating content involving identifiable individuals.
- Not use AI for personal projects on company devices or networks.
- Ensure AI use aligns with company values, standards, and legal obligations.

Training and Awareness

The company may provide training on responsible AI use during onboarding and when policies or tools change. Employees are encouraged to raise concerns about fairness, bias, or risks with their manager.

Monitoring and Policy Breach

The company may review AI use and outputs to ensure compliance with this policy in accordance with privacy law.

Misuse may result in disciplinary action, up to and including dismissal. Any suspected data breach must be reported immediately.

Policy Review

This policy may be amended, updated, or discontinued at the company's discretion.