Generative Artificial Intelligence

Te Kāwanatanga o Aotearoa
New Zealand Government

SYSTEM LEADERS' GUIDANCE FOR USE OF GEN-AI ACROSS THE NEW ZEALAND PUBLIC SERVICE

What is AI and Generative AI (GenAI)?

AI: engineered systems that can generate outputs for key objectives without explicit programming.
Machine/deep learning: ML trains machines to make decisions. DL is more specialised, typically involving more complex data and decisions.
Gen-AI: uses prompts to generate outputs closely resembling human-created content. ChatGPT is a well known free GenAI tool.

What is the purpose of this guide and who is it for?

- GenAI tools present opportunities and risks, and the interest in them is increasing.
- Not all GenAI tools are equal. Free and paid GenAI tools come with their own sets of risks. Generally, we encourage agencies seeking to use GenAI for its benefits to understand the necessity for it, and to actively manage the risks.
- This guide is designed to support AI leaders and practitioners to make informed decisions about using GenAI. It will be updated as risks are better understood.
- System Leads are working with Ministers on options to address broader AI issues.
- Refer to the AI advice document supporting this A3 for more advice/case studies.

We strongly recommend that you:

Don't use GenAI for data classified at SENSITIVE or above.

Don't input or use personal data in GenAI tools if they are external to your environment.

We also recommend that you:

Avoid inputting personal data into GenAI tools in your network, unless (a) it isn't possible to use non-personal or synthetic data; and (b) potential harms have been addressed.

Prevent AI from being used as shadow IT. Be aware that free GenAI may carry higher risk, and paid GenAI also carries risk. We recommend blocking GenAI tools until this guide is applied.

Avoid inputting into GenAI tools any information that would be withheld under the Official Information Act.

Avoid using GenAI for business-critical information, systems or public-facing channels.

Understand the benefits, for your agency and for all New Zealanders. We consider these could be:

Efficiency and productivity through process simplification and automation

Improved service design and delivery through targeting and personalisation

Enhanced cyber monitoring and defence through advanced predictive analysis and threat detection.

Innovation from optimisation and access to insight that is based on significantly larger volumes of data.

Improved policy through better options analysis and ability to explain complex concepts in plain English.

10 do's for trustworthy use of GenAI for the Public Service.

Use GenAI tools responsibly

Robustly govern the use of GenAI – consider your governance system and obtain senior approval of GenAI decisions. Develop an AI policy for your agency and share it with the Government Chief Privacy Officer.

Assess and manage for privacy risk – take all necessary steps to protect privacy. This includes undertaking and getting senior approval of a robust privacy impact assessment for any testing or use of GenAI.

Assess and control for security risk – GenAI can increase risk of data or security breaches, so undertake approved security risk assessments. Opt out of GenAI tools retaining your data for training, if possible.

Consider Te Tiriti – work with Iwi Māori where GenAI may be being used for Māori data, and/or its use may impact Māori, including services to Māori.

Use AI ethically and ensure accuracy – GenAI can perpetuate bias and mis/dis information. Understand the limitations and take active steps to check for accuracy when using GenAI outputs, to avoid harm.

Be accountable – always ensure accountable humans are making the decisions in respect of applying or using GenAI outputs, and that the decision-makers have the necessary authority and capability.

Check and test GenAI tools

Be transparent, including to the Public – be open and transparent in terms of what GenAI is being used for and why. Ensure processes are in place to respond to citizen requests to access/correct information.

Exercise caution when using open-source AI – be aware of the known security, quality, intellectual property and supply chain risks of open-source AI and mitigate risks where possible before using AI tools.

Apply Government's procurement principles – GenAI can increase risk of vendor lock-in, and exposure if providers are using GenAI in their services to you. Use the procurement rules when sourcing GenAI tools.

Test safely – create guardrails and space, like sandboxes, for your teams safely to trial and learn to use genAI. Use lower-risk datasets and robustly test outputs before they are deployed.