Ministry Guidelines for using Artificial Intelligence and Generative AI

This page outlines clear guidelines for what Ministry people can and cannot do to protect data privacy, ensure compliance and build and maintain public trust.

As Artificial Intelligence (AI) systems and Generative AI (GenAI) continue to evolve rapidly our standard and guidance will continue to adapt alongside these advancements and public expectations.

On this page:

- What is AI?
- Why do we need to be vigilant when using AI and GenAI?
- Approved tools
- Blocked or prohibited tools
- Can I use other AI tools?
- Key risks to be aware off when using AI or GenAI at work
- What you can and cannot do with AI/GenAI tools at work
- Steps to using AI/GenAI safely at work

What is AI?

- **Artificial Intelligence (AI)** refers to computer systems that perform tasks requiring human-like intelligence, such as learning and problem solving.
- **Generative AI (GenAI)** is a type of AI that creates new content, like text, images, and videos, by learning from data.

Why do we need to be vigilant when using AI and GenAI?

The Ministry has an obligation under legislation to protect the individual's sensitive data and our confidential information. Therefore, we should be vigilant about what information is being input into any technology, including AI or GenAI tools.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

You are responsible for keeping information secure and using Ministry ICT appropriately, in line with the Information and Communication (ICT) use Policy.

Approved tools

The only GenAI tool approved by the Ministry is Microsoft Copilot Chat. It is available for web searches and to input information that is marked **UNCLASSIFIED, IN-CONFIDENCE or is in in the public domain.** Always ensure you are logged in to Copilot with your Ministry account. There are AI drop-in sessions that you can join for further guidance on how to use Microsoft Copilot at work.

The Ministry is exploring the use and approval of other AI tools. If you are interested in using other technology, then please follow the Matihiko Technology Needs Assessment process.

Blocked or prohibited tools

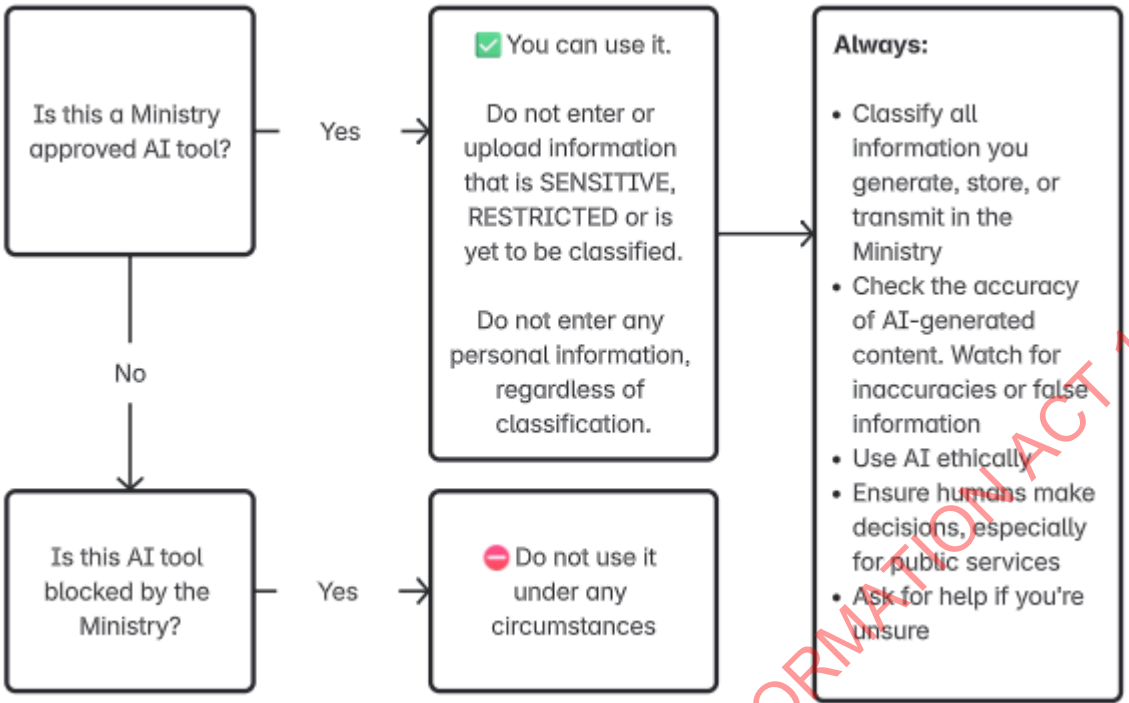
You **must not** use or access blocked tools or technologies, including AI, on Ministry devices or with Ministry data and information. These tools are blocked because they pose a risk to Ministry systems and information, or we have a suitable alternative available within the Ministry. If you attempt to access a blocked tool, you'll see a warning or splash page letting you know it's been restricted.

The Ministry has blocked several well known AI and Gen AI websites such as ChatGPT, Grok, Gemini, Perplexity and Claude.

Can I use other AI tools?

This decision tree is here to help you determine the most appropriate tool for your task, whether that's Microsoft Copilot or another AI tool. While external tools can be useful, they come with additional risks. Always consider the type of information you're working with.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



Key risks to be aware off when using AI and GenAI at work

1. **Risks of security, privacy** and exposing confidential or sensitive data.
    - AI and GenAI tools may not have security measures to protect data or adhere to industry standards.
    - GenAI tools might expose data to misuse or security breaches.
    - AI and generative tools may inadvertently expose classified, personal or sensitive information. Only use publicly accessible information in AI tools.
2. **Risk of accuracy issues:** GenAI tools can generate content, such as text, images, audio, and video, that may look or sound convincing but might not always be accurate. It's important to double-check everything created by GenAI. Consider setting up a peer review process within your team where AI-generated content is fact-checked by at least one other person.
3. **Risk of bias**: GenAI tools can reflect biases based on the data they're trained on. Always review results for fairness.

What you can and cannot do with AI and GenAI tools at work

- **Do**:
    - Use them only for information marked as **UNCLASSIFIED, IN-CONFIDENCE or in the public domain.**

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

    - Check the accuracy of AI generated content. AI hallucinations are instances where generated information appears credible but is entirely false. Note that this could take more effort than doing it yourself.
    - Consult with the Privacy Team for advice and to complete a Privacy Assessment if you think you may need to use personal information (privacyteam.advice@education.govt.nz).
    - Be careful when copying and pasting information into AI tools. Type directly into them.
    - Use AI ethically. If unsure, consult Ethics Advisory (ethics@education.govt.nz).
- **Don't**:
    - Input data classified as **SENSITIVE, RESTRICTED, or yet to be classified**.
    - Input personally identifiable information (e.g. name, date of birth, address).
    - Input anything that might need withholding under the Official Information Act or relevant legislation.
    - Input anything that is to be discussed with a Minister, is pending a decision from them, or would need their approval to be released.
    - Use AI for business-critical information, systems or public facing channels.
    - Use AI to make decisions, especially for any public services.
    - Use AI for code generation in a production environment or with production data unless:
        - The code is peer-reviewed by a skilled human developer, including vulnerability checks.
        - The code is fully tested using appropriate code vulnerability scanning tools.

Steps to using AI and GenAI safely at work

1. **Get Approval**: Inform your manager before using any new digital tools, including AI and GenAI.
2. **Check the tool is approved for use**: Contact the Service Desk Portal if you aren't sure. The only GenAI tool approved by the Ministry is Microsoft Copilot Chat.
3. **Follow the Guidelines** as outlined on this page and detailed in the Artificial Intelligence and Generative AI Standard.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982