

Using generative artificial intelligence in the Scottish Government

Scottish Government policy on artificial intelligence (AI)

Generative artificial intelligence (AI) describes any type of artificial intelligence that can be used to create new text, images, video, audio or code. Large language models (LLMs) are part of this category of AI and produce text outputs.

ChatGPT and Google's Gemini are publicly available web-based versions of generative AI which use an LLM. They allow users to enter text and seek a view from the system, or to ask the system to create output based on a given subject. You can also ask it to summarise long articles, get an answer of a specific length to a question, or have code written for a described function.

We encourage all colleagues to experiment and try different AI tools but we also have a duty to protect our data and ensure safe use of AI technologies.

These rules are essential for using AI safely:

1. Do not use personal data in generative AI tools. This ensures we do not share personally identifiable information, protecting staff and the wider Scottish public from having data collected by generative AI products.
2. Do not use sensitive information in generative AI tools. Be aware that non personal data can be sensitive, and will not always be protected by data protection regulation. This could be details of an embargoed press release, creative material designed as part of a campaign or the text of a ministerial announcement. Do not share anything you would not be happy to share with a member of the public.
3. Do not use terms which could infer future government policy or thinking in generative AI tools. For example, you should not ask questions such as 'what might happen if the Scottish Government set the driving age to 12?' Generative AI works like a giant database, and a search term like this links the Scottish Government with the concept of driving at 12. This means similar text could be returned as a search result in other users' searches and could potentially link the Scottish Government to outputs that are insensitive or inappropriate.
4. When using generative AI, check the output carefully before sharing or relying on the search output. With appropriate care and consideration, generative AI can be helpful and assist with your work, however, you should be cautious and circumspect in your approach.

This guidance covers LLMs such as ChatGPT, Gemini and BLOOM, and systems generating images based on text, such as DALL-E, Stable Diffusion and Midjourney.

To discuss specific examples of using AI, contact the AI policy team.

UK Government guidance on using generative AI

The UK Government has released a framework for the use of generative AI, which is based on 10 key principles:

1. You know what generative AI is and what its limitations are.

2. You use generative AI lawfully, ethically and responsibly.
3. You know how to keep generative AI tools secure.
4. You have meaningful human control at the right stage.
5. You understand how to manage the full generative AI lifecycle.
6. You use the right tool for the job.
7. You are open and collaborative.
8. You work with commercial colleagues from the start.
9. You have the skills and expertise that you need to build and use generative AI.
10. You use these principles alongside your organisation's policies and have the right assurance in place.

The framework aims to help civil servants understand generative AI and to guide anyone building generative AI solutions. Most importantly, the framework lays out what must be considered to use generative AI safely and responsibly.

Using AI systems safely and securely

Artificial intelligence (AI) has quickly become a technological advance that offers great opportunities, but also carries significant risks in its use. It's important to understand these risks before using AI systems at work.

The main risks to consider are:

1. disclosure of information submitted to AI systems
2. the accuracy of AI responses

The main AI systems on offer all use information provided by users in their free offerings, and some in their paid-for versions, to train their AI models. This means that control of who can access that information has been lost once it's been submitted to that AI system.

Data entered into AI systems is generally stored outside of the European Economic Area (EEA), mainly in the United States. Some of these vendors may have agreements or mechanisms in place to help comply with General Data Protection Regulation (GDPR). However, others, such as OpenAI's Data Protection Addendum (DPA) for ChatGPT, only apply to countries within the European Union (EU) or European Economic Area (EEA).

Paid for versions of some AI systems, such as ChatGPT Enterprise, do offer a greater level of control of data. But you should not assume that paying for a service means that data is fully under your control, or is processed in compliance with data protection laws.

AI vendors have made the risks around submitting sensitive information to their systems clear. Open AI, Microsoft and Anthropic have all advised that you do not share sensitive information or process personal data on ChatGPT, CoPilot or Anthropic. These AI vendors also advise that any information provided should be fact checked before being used. This is because these AI systems will occasionally produce responses that are incorrect, misleading, incomplete or inappropriate. This result from AI systems is known as 'hallucinating' information.

Precautions to take

Given the warnings provided, any decisions to use a paid for access model should consider whether there are sufficient safeguards around access to information submitted to that AI system.

You must also fact check any information supplied by an AI system, as there is no other way to determine which answers are accurate, and which are 'hallucinated'.