Generative AI Policy

Version 2.0

02 July 2025

1 Purpose and scope

Generative AI presents a real opportunity for us to deliver more for our clients and work more efficiently. Our ambition is to be at the forefront of the use of Generative AI in economic consulting, with these tools used by all staff in the most effective way possible. The aim of this policy is not to overly restrict the use of Generative AI, and we would encourage anyone who feels that their use of these tools is being held back to contact the Head of Data Science (David Dorrell) to discuss how the firm can help.

However, these tools do carry risks that require responsible management, and are subject to regulations such as the EU AI Act and GDPR. This document sets out the principles that all Frontier staff must follow when using Generative AI tools.

While this policy covers the most likely use-cases at Frontier, it is not possible to plan for every eventuality. If you are uncertain about whether Generative AI can be used for a given application, please contact both:

- IT Security and Data Protection Manager (rob.ding@frontier-economics.com)
- Head of Data Science (david.dorrell@frontier-economics.com)

2 Scope and definitions

This policy applies to all Frontier Economics staff. This includes permanent and temporary employees, contractors, associates, Research Assistants and interns.

'**Generative AI**' refers to systems capable of producing new content (text, code, images, etc.) based on training data. Examples include (but are not limited to):

- Large language model chat tools (e.g. ChatGPT, Edge Copilot, DeepSeek)[1]
- AI image generators (e.g. Midjourney, DALL-E)
- AI note-takers

[1] Generative AI tools like DeepSeek which are not on the list of approved tools below are prohibited for use at Frontier.

3 Training

All Frontier employees must complete annual Generative AI security and compliance training modules, which include an overview of this policy. Frontier provides additional training on how to make the most effective use of Generative AI, and all staff using Generative AI are highly encouraged to make use of this.

4 Generative AI tools within Frontier

Frontier provides access to the following Generative AI tools:

- **ChatGPT Enterprise** (you *must* be logged in to Frontier's account – this is the case if you see the message 'OpenAI doesn't use Frontier Economics Enterprise workspace data to train its models' at the bottom of the screen).
- **GitHub Copilot** within the Frontier Economics Organisation on GitHub.

Please contact the IT Helpdesk to access these tools. We understand that some staff may need to use more specialist tools. If you have a requirement to use a Generative AI tool not listed here, please contact David Dorrell and Rob Ding. Do not use a tool not listed above until they have confirmed in writing that this is OK.

These tools may be used for all Frontier work (whether internal or using client data) unless:

- A Director or AD has explicitly restricted the use of Generative AI for a particular project or part of a project. Annex A describes when this may be required – for example if a client has restricted the use of Generative AI or hosting data on a EU/UK 'cloud' platform.
- the use of Generative AI would be prohibited, or considered high risk, by the EU AI act (see Annex B for a description of the uses this covers).

All usage of Generative AI tools should be in line with the best practices for using Generative AI described in section 5.

A Data Protection Impact Assessment (DPIA) may need to be carried out when a data processing activity could result in a high risk to the rights and freedoms of individuals. This is a requirement under the UK & EU GDPR, intended to help organisations identify, assess, and mitigate data protection risks early in a project lifecycle. Examples of high risk data processing activities include automated hiring tools that screen candidates without human intervention, processing data on racial or ethnic origin, political opinions, or religious beliefs at scale or the use of new or innovative technology such as deploying AI or machine learning to make decisions about individuals.

5 General best practice for using Generative AI

This section describes the best practice which all staff should use to mitigate key risks from the use of Generative AI.

Table 1 Practices for using Generative AI

Risk	Controls to mitigate risk
Generative AI output contains 'hallucinations' (seemingly plausible but incorrect output, including invented 'sources')	Do not provide Generative AI output directly to clients without human review – including checking of sources, and having a subject matter expert review the content. If for any reason this is not practical, the content must be prominently flagged as having been produced by AI and subject to these potential issues.
Generative AI output infringes copyright	Review output, checking if any content that could be a verbatim quote needs sourcing. Ensure that imagery created with Generative AI does not include visible brand logos etc.
Analysis or source code produced by generative AI contains bugs or does not do what is expected	Quantitative analysis carried out by Generative AI should be subject to at least the same level of scrutiny as code written by a human. Frontier's Quality Management strategy includes guidance – this might include having someone reviewing the code, a 'sense-check' of outputs by a subject matter expert, and appropriate unit tests.
Decisions made by generative AI adversely affect individuals	Avoid fully automated decision-making and ensure that human reviewers validate or can override automated decisions. Provide clear, intelligible explanations to data subjects about the logic, significance, and consequences of automated decisions. Implement fairness and bias controls and offer individuals a right to object or seek human intervention.

6 Annex A: Guidance for Directors and Associate Directors

Frontier's Generative AI policy permits staff to use certain Generative AI tools on project work *unless told otherwise by an Associate Director or Director*. The responsibility is therefore on the AD/D to communicate if this is not the case. This should be done by:

- Informing all staff by email as they join the project (and asking them to confirm by replying).
- Adding the suffix " (NO AI)" to all folders containing information that Generative AI should not be used on.

Evidence should be retained in the project folder.

Frontier provides its staff with secure Enterprise-grade Generative AI tools which can help us produce high quality work, efficiently. We should not seek to restrict the use of these tools unnecessarily. However, there may be certain instances where their use is inappropriate.

You should prohibit the use of Generative AI entirely on projects where the project/framework contract, NDA or other relevant legal agreements contain any of the following conditions (Frontier's standard Ts & Cs do *not* contain these conditions), or the client has informed you of:

- A prohibition on confidential data being hosted on third party 'cloud' services; or
- a prohibition on the use of Generative AI.

If you need to restrict the use of Generative AI for any other reason, avoid making the restriction too broad. If a client has restricted the use of Generative AI but you feel it would help deliver higher quality work at lower cost then it may be worth trying to push back on this. Please contact Rob Ding and David Dorrell if further guidance is required.

7 Annex B: Uses restricted by the EU AI Act

This annex provides a high-level summary of uses of AI which the EU AI Act prohibits, as well as the uses it deems to be 'high risk' and which are also prohibited at Frontier. Please contact Rob Ding if further guidance is required.

Prohibited uses include:

- **Tools which deploy subliminal techniques with the objective of distorting people's behaviour to make a decision which is reasonably likely to cause harm.** For example, we could not provide a tool to a client which uses AI techniques to craft sales messages in a misleading way.
- **Tools which exploit the vulnerabilities of people in a way which is reasonably likely to cause harm**. For example, we could not provide a tool to a client which uses AI techniques to increase prices charged to groups such as elderly people.
- **The use of AI systems for evaluation or classification of people based on social behaviour or personal characteristics, with the social score leading to detrimental or unfavourable treatment.** For example, we could not work on a 'social credit' scoring algorithm for a state.
- **The use of AI systems for making risk assessments of the risk of people committing criminal offences (unless the AI system is used to support human assessment).** For example, we could not produce a system which is intended to identify the likelihood of individuals committing crimes, unless it is clear that the system is only an input to further human assessment.
- **AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.** For example, we could not implement a CCTV system which builds a facial recognition database.
- **The use of AI systems to infer emotions of people at work.**
- **Systems that categorise people based on biometric data to deduce sensitive information about them**. For example, we could not work on an algorithm that uses inputs such as body shape or keystrokes to predict behavioural or personality traits.

‘High risk’ uses (which are also prohibited at Frontier) include:

- **Systems intended to be used as a safety component of a product.**
- **Systems used as safety components in the management and operation of critical infrastructure**. For example, we could not provide an AI system which is required to ensure that energy, telecommunications, water or transport systems can run.
- **Systems used to determine access to education or carry out educational evaluations.**
- **Systems used for recruitment**. For example, we could not use AI tools to assess applications to Frontier.
- **Systems used to evaluate the eligibility of individuals for public services, credit, or life insurance.** For example, we could not work on an AI model which would be used to provide credit scores.
- **Systems used on behalf of law enforcement or migration, asylum and border control.**
- **Systems used for the administration of justice and democratic processes.**

Revision history

Version No	Date	Reason and change made	Authored by	Reviewed by
1.0	8 Nov 2023	Initial version of policy	David Dorrell	
1.1	14 Jan 2025	Minor edits to reflect new tools	David Dorrell	
2.0	2 Jul 2025	Re-write, allowing some Client Information to be used with enterprise-grade AI tools	Alex Whittaker David Dorrell Rob Ding	Damien O'Flaherty