IB1 Research Guide: Using Large Language Models

2025-11-27

ib1.org

What are Large Language Models (LLMs)?

Recent progress in AI has largely been focused on Large Language Models (LLMs), capable of tasks such as natural language processing and generating content.

LLMs such as ChatGPT and Claude are increasingly used to support research. LLMs are a type of Generative AI built on Deep Learning techniques. Other forms of AI have been in wide use for decades such as traditional Deep Learning used for classification or prediction, and Reinforcement Learning systems that learn through trial and error.

LLMs aim to generate a human-readable response based upon the input provided e.g. a question or prompt. LLMs generate the response by predicting the most likely next word in a sequence using patterns learned from their training data. They can help in analysis of existing content, generating computer code, and drafting text-based content. This is done primarily in the form of "chats" where a user asks a series of prompts or questions and the LLM provides a response based on those questions.

LLMs are probabilistic and generate plausible text rather than verified facts. They should not be used as a search engine or authoritative sources but can be used to explore ideas or in identifying areas for deeper investigation.

mySociety AI Framework

mySociety has created an AI framework including guiding principles and questions for using LLMs and AI as part of a mySociety service or output.

Key principles from the mySociety AI framework are:

- Practical – does it solve a real problem for us or our users?
- Societal – does it plausibly result in the kind of social change we want, and have we mitigated change we don't want?
- Legal/ethical – does our use of the tools match up to our wider standards and obligations?
- Reputational – does using this harm how others view us or our services?
- Infrastructural – have we properly considered the costs and benefits over time?
- Environmental – have we specifically accounted for environmental costs?

Icebreaker One has adopted this document and these principles as the basis for internal guidance on using LLMs and AI tools for research responsibly.

Icebreaker One additions to mySociety AI framework

Icebreaker One's guidance for researchers is provided below, adding principles on top of the **mySociety AI Framework:**

- Transparency
    - Are we being transparent about which LLM model is being used?
    - Are we being transparent about the prompts used to generate any outputs?
- Replicability
    - Can another researcher replicate our use of LLMs by using the same prompts and LLM model?
    - Have we documented the chat (series of prompts), LLM model and LLM version used, so that others can replicate our approach even if identical outputs can't be reproduced?
- Domain expertise
    - Have we got enough domain expertise to review the outputs of an LLM?
    - Have we done an expert review of the output of an LLM before using the content?
- Check every citation
    - Have we verified that every citation, website, and reference provided by an LLM is both valid and relevant to the prompt, recognising that LLMs can sometimes "hallucinate" sources such as research papers and legal documents?
- Text not data analysis
    - Have we used the LLM appropriately? (e.g for complex text analysis, reviewing long, text-based research documents)
    - Have we avoided using the LLM for data analysis which it is not designed to perform?
    - Have we ensured that any use of an LLM to identify potential data sources or references is appropriate and well justified?
- Data and privacy
    - Have we opted out of allowing the LLM to use our prompts or data for future model training, where appropriate?
    - Have we ensured that we have not uploaded any data that must be retained in certain jurisdictions or subject to data residency requirements?
    - Have we reviewed the LLM usage with respect to organisational data policies?

Practical considerations for researchers

This section contains a number of practical steps that can be taken to put the mySociety and Icebreaker One principles into practice.

Save the model and the prompts with any responses in its own document as it is a source document

When using a tool such as ChatGPT, the entire chat (series of prompts) should be saved to a separate document, along with the LLM name and LLM model used. Keep it separate from other notes or documents so that it can be identified as an LLM generated document separate from other content.

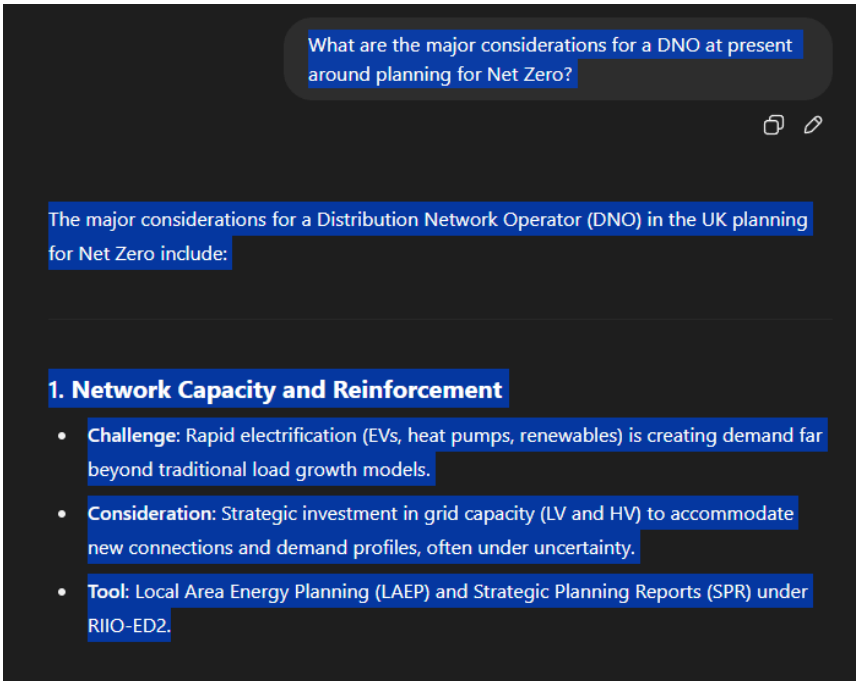
When saving the document it is useful to add an identifier to the title that clearly marks it as an LLM document. For example, adding "#LLM" to all LLM generated content would allow it to be easily identified from just the title, as well as easily searched for within the document repository e.g. Google Drive. Adding the LLM name and model would provide additional context.

e.g. "#LLM #ChatGPT #model4o".

Use copy and paste instead of print

Using the print function can result in prompts and responses not being saved correctly with some LLM tools. The current best practice is to manually select all the prompts and outputs in the chat interface. If the chat is long, then it can produce a very big document.

e.g.



This copy and paste uses ChatGPT as an example, and will output in a text-based form that can easily be reviewed outside the tool.

The above screenshot of the text copied outputs the below content in an HTML based document such as if using Google Docs:

> What are the major considerations for a DNO at present around planning for Net Zero?
>
> ChatGPT said: The major considerations for a Distribution Network Operator (DNO) in the UK planning for Net Zero include:
>
> 1. Network Capacity and ReinforcementChallenge: Rapid electrification (EVs, heat pumps, renewables) is creating demand far beyond traditional load growth models.
>
> Consideration: Strategic investment in grid capacity (LV and HV) to accommodate new connections and demand profiles, often under uncertainty.
>
> Tool: Local Area Energy Planning (LAEP) and Strategic Planning Reports (SPR) under RIIO-ED2.

Maintaining privacy and confidentiality

LLMs are generally services provided over the internet. The servers that process data may be in different countries and each LLM will have different policies as to how they use the prompt data provided.

It is important to be aware of jurisdiction when uploading any data (prompts or documents) that may be confidential. Consider downloading and using a local LLM using a tool like LM Studio or similar where this may be an issue. It is likely to be slower to generate information but will limit impact where data privacy is a consideration.

It is important to check settings for each LLM, especially to opt out of allowing an LLM to use the prompt data provided for future model training.

Take care that your account is private and that sharing chats is done with privacy in mind. Where possible, avoid making any LLM chats public via sharing a link to a chat or similar. Copy and paste is more secure under this scenario.

Considerations around AI/LLM energy usage

At present it is not clear how much energy is used to create the LLM models, or how much is used in making queries of these models. The current major LLM services do not provide the information needed to assess this adequately. The **IEA expects electricity demand from data centres to nearly triple by 2035** primarily due to the growth in AI.

One approach to ensuring that usage of LLMs uses renewable energy would be to use an LLM model running on a provider like the German **WindCores** who put data centres in wind turbines. There are a number of models that could be implemented like this, but the technical considerations are significantly different to using an LLM service such as ChatGPT or similar.

Regarding model creation, potentially the best choice is Claude which runs on AWS, and AWS has a commitment to be 100% energy neutral. Using Claude may be an indirect way to try to limit energy impacts of using LLMs.

List of major LLM tools

Below is a non-exhaustive list of major LLM tools with no preference asserted. It is important to check each provider's data and privacy policies before use.

- LM Studio
    - **https://lmstudio.ai/**
    - Run models on your machine rather than use a service meaning data security is easier to manage
    - Can download many different models, including some listed below
    - Relatively slow compared to using the services but may be useful to avoid negative impacts such as energy usage for some tasks
- ChatGPT
    - **https://chatgpt.com**
    - Operated by OpenAI (US)
    - The most well known LLM
- Claude
    - **https://claude.ai/**
    - LLM from Anthropic (US) and runs on AWS infrastructure
- Gemini
    - **https://gemini.google.com/**
    - Google (US) LLM solution
- Copilot
    - **https://copilot.microsoft.com/**
    - Microsoft (US) LLM
    - GitHub (part of Microsoft) created the **GitHub Copilot** which is a coding based LLM
- Grok AI (xAI)
    - **https://x.ai/**

    - Elon Musk owns xAI (US)
    - Alleged bias in results
- Deepseek
    - **https://www.deepseek.com/en**
    - LLM produced in China
- Perplexity AI
    - **https://www.perplexity.ai/**
    - US-based LLM tool designed for research and information retrieval
    - Blends search and generative functions