Prompt Library Launch Event

EDLAB
09 october 2024



Outline of the Event

11.00	Workshop	
	> Introduction	Gaby
	Introducing GenAi	Michalina
	Various Tools and Ways how to protect your privacy	Irene
	Exercise 1: Getting started	Irene
	How to prompt	Michalina
	Exercise 2: Prompting	Michalina
	Al prompt engineering skills module	Noah
	Closure.	
13:00	Lunchbreak	
13.45	Panel discussion	
15:00	Closure	



The Prompt Library

A Prompt Library is a collation of prompt templates.

- What is a prompt?
 - A prompt is an instruction given to generative AI to guide it in producing a specific response.

- Why a Prompt Library?
 - To inspire and give a starting point.



But First Things First

What is generative AI? Why does prompting matter?

What tools are out there? How to protect you privacy?

How to prompt effectively, and use the Prompt Library?

What is generative AI?

Artificial Intelligence...





is an umbrella term for technologies that mimic human intelligence.



How Supervised Learning Works

Movies you watched: Comedy

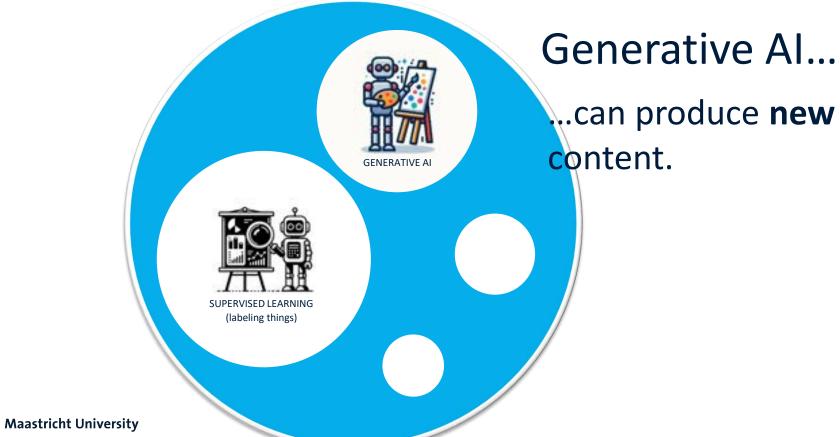


Comedy

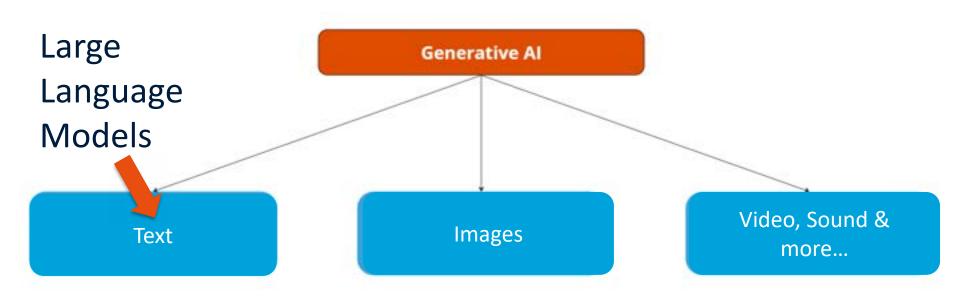




What is generative AI?



Generative Al can generate:

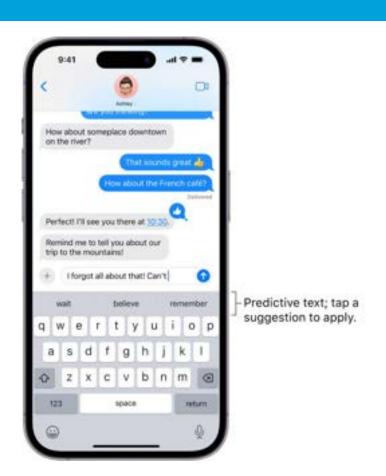


How Large Language Models Work

In the morning, I like to drink a cup of <u>coffee</u>

Many businesses use <u>social</u>media for marketing.

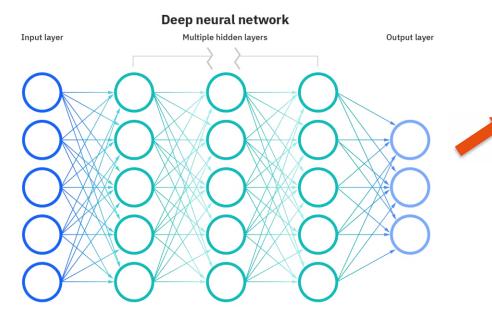
This, but BETTER!



Why does prompting matter?

Prompt

"What is the capital of France?"



Al's response

"Paris"

It uses learned weights to capture the pattern: "capital" is often followed by the name of a city, and "France" often pairs with "Paris."



Why does prompting matter?

Give me three beverage suggestions.



Give me three beverage suggestions for my daughter's 6th birthday party. She loves Disney princesses and purple color.



- 1. Grape juice with sparkling water
- 2. Lemonade with food coloring and edible glitter
- 3. Mix berry smoothie

Add princess straws!

Why does prompting matter?

Because context matters!

And so does the clarity of what we are asking for.

More on that later...

And Next...

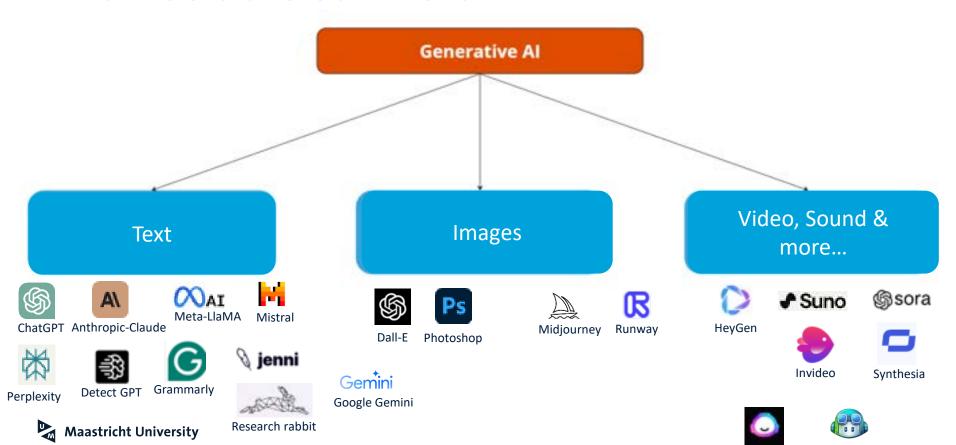
What is generative AI? Why does prompting matter?

What tools are out there? How to protect you privacy?

How to prompt effectively, and use the Prompt Library?



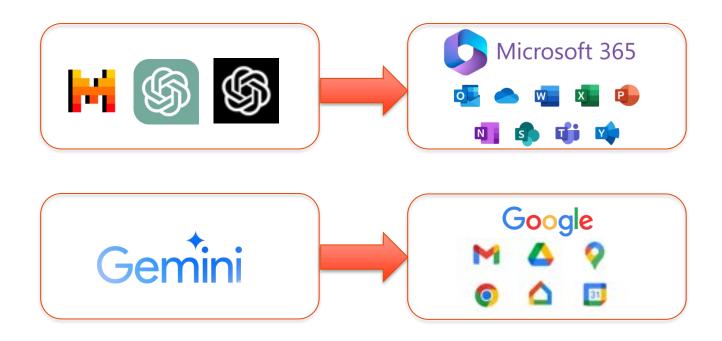
What tools are out there?



GitHub Copilot

Jasper

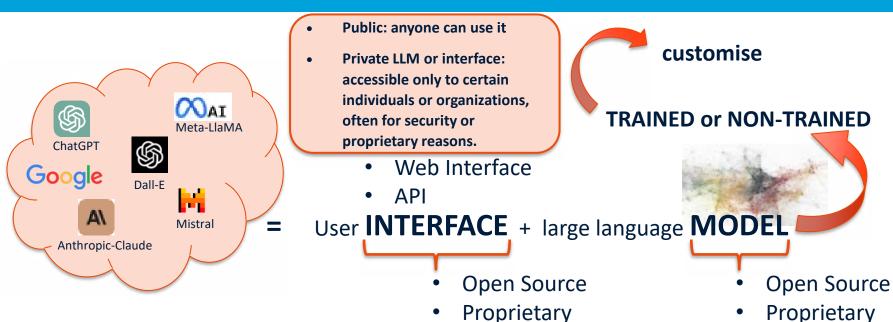
What tools are out there?



For example:



Proprietary vs **Open Source** & **Private** vs **Public**



- **Open Source**: the source code of the model is available for anyone to inspect, modify, and distribute, allows for transparency and community contributions.
- **Proprietary**: the source code is owned by an individual or organization and is not available for public use or modification, developed to maintain control over the technology.

Proprietary vs **Open Source** & **Private** vs **Public**

User INTERFACE + large language MODEL

- Open Source
- Proprietary

- Open Source
- Proprietary
- "public" and "private" describe the accessibility of the model or interface,
 - "open source" and "proprietary" describe the availability and control of the source code.
- They can intersect in various ways but are not synonymous.



≠ Gratis

Maastricht University

Awareness of risks









Data: Know what you share

Examples of information better not to share

- 1. Login data and passwords
- **2. Personal data:** Names, addresses, phone numbers, email addresses, dates of birth, student numbers, photos, voice recordings
- **3. Financial data:** Credit card numbers, bank account numbers, quotes, financial transactions, salary information
- **4. Health information:** Medical records, diagnostic data, insurance information, mental health complaints
- **5. Business-sensitive information:** Contracts, minutes, agendas, presentations, Excel sheets



How to protect your privacy?

Security & Privacy Best Practices

- Use Strong Passwords
 Ensure your ChatGPT Plus account is protected by a strong, unique password.
- Two-Factor Authentication (2FA) Enable 2FA for enhanced security.
- Limit Data Sharing

 Avoid sharing personal, sensitive or financial information during your interactions.
- Regularly Review Activity
 Check your account for any unusual activity and log out from unused devices.

How to protect your privacy?

Security & Privacy Settings

Disable model training

Your interactions are not used to train and improve the model reducing the amount of personal data being processed and stored.

Enable Multi Factor Authentication

Adding this secondary factor to your username/password protects your privacy.

Disable Memory

Ensures that no data from your previous interactions is stored, reducing the risk of unwanted data retention or breaches

Activity

Setting Up an Account



Disable model training

Click on your profile icon at the top right of the ChatGPT interface

- Navigate to Settings / Instellingen.
- Click on Data Controls / Gegevensbeheer.
- Set the option Improve the model for everyone to Off.

Enable MFA

Click on your profile icon at the top right of the ChatGPT interface

- Navigate to Settings / Instellingen.
- Click on Data Controls / Gegevensbeheer.
- Set the option Improve the model for everyone to Off.

You are asked to login to your account

After successful login this dialog appears:



Enable MFA

Secure Your Account

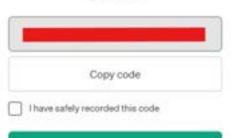
Scan the QR Code below using your preferred authenticator app and then enter the provided onetime code below. Enter your one-time code* Continue

- Open the Authenticator App on your Mobile phone.
- Click on + to add a Work or School Account.
- Scan the QR code.
- A profile for OpenAI is now added to your Authenticator app.
- Enter the one-time code from the app.
- Store the recovery code in a safe place!

Enable MFA

Almost There!

Copy this recovery code and keep it somewhere safe. You'll need it if you ever need to log in without your device.





- Store the recovery code in a safe place!
- MFA is now enabled on your ChatGPT Plus account.

Disable memory

Click on your profile icon at the top right of the ChatGPT interface

- Navigate to Settings / Instellingen.
- Click on Personalisation / Personalisatie.
- Toggle the Enable Memory switch to OFF.
- Confirm this choice when prompted, ensuring the system will not store conversations between sessions.

Other settings

Profile Configuration

A customized profile allows ChatGPT to generate responses aligned with your professional background and needs, providing more relevant and structured feedback.

- Navigate to **Settings / Instellingen**.
- Click on Personalisation / Personalisatie.
- Set the option Profile Configuration/Aangepaste instructies to On.

https://help.openai.com/en/articles/8096356-custom-instructions-for-chatgpt

Finally!

What is generative AI? Why does prompting matter?

What tools are out there? How to protect you privacy?

How to prompt effectively, and use the Prompt Library?



Why a Prompt Library?

- Prompting is a learnable skill; learn to prompt based on examples
- Prompt templates might help getting started and inspire
- A place to share actionable ideas on how to use generative AI in education

Prompt Library Launch



www.maastrichtuniversity.nl/prompt-library

How to prompt effectively?

More information



More individualized answers

Prompting is a building process





How to prompt effectively?

Structure

Logical order
Numbering
Headings/delimiters

Scope

Context Boundary settings

Instruction

Specific Unambiguous

Format

Description of the output

Validation

Recursion
Iterative prompting
Questions, etc.

Example

Same us...



Prompting methods as in the Prompt Library.

Prompt: Improve text step-by-step



THE BASIC RULES OF PROMPTING

A prompt must be **structured.**

"Structured" refers to the organization and logical arrangement of the information within a prompt. A structured prompt is one where the information is presented in a coherent, logical order, making it easy for an AI model to follow the instructions.

An AI model assimilates information in the order it is written. Therefore, a change in the order of the text in a prompt can lead to very different results in terms of the quality of the model's response.

A prompt must be **specific.**

"Specific" refers to providing detailed, clear, and precise information in a prompt. A specific prompt includes all relevant details that might be needed to determine the response.

An AI model predicts the most accurate response based on the prompt provided. Therefore, the more detailed the instructions, the better tailored the response will be.

A prompt must be unambiguous.

"Without ambiguity," on the other hand, focuses on ensuring that the prompt cannot be interpreted in more than one way, eliminating any potential confusion about what is being requested.

An AI model operates within the limits of what it is told.
Therefore, if instructions are open to multiple interpretations, the resulting interpretation may not align with your expectations.

Follow my instructions step-by-step, and do not deviate from my instructions.

Context: % add context %

Task:

- 1. Ask me what text I need editing. Wait for my reply. Do not continue until I reply.
- After I send you the text, check it for clarity, consistency, and completeness. Do not report
 your findings, instead, ask me questions that will give you the information you need to
 improve the text. Consider the context described above between %%. Wait for my reply to
 your questions. Do not continue until I reply.
- 3. Based on my input, adjust the text to be clear, consistent, and complete. Highlight the changes you made by making the changed text bold. Do not make any other changes to the text. Show me the adjusted text. Wait for my reply.
- 4. Review the adjusted text. Pay attention to the following:
 - 4.1. Poorly structured sentences and suboptimal word choices.
 - 4.2. Consistency with the desired tone. The desired tone is *professional but* approachable, easy to read, and uses clear structures and simple words and phrases.
 - 4.3. Spelling and grammar.
- 5. Do not rewrite the text. Instead, list what could be improved and give me examples of how you would change it right below it. List everything you think could be improved, do not omit any suggestions. Number the elements on the list.

Clear Objective & Context

Begin with context that sets the stage for what you are asking; you can do it by assigning a persona (Act as...).

Clearly state the main objective of the prompt. This helps to orient the model and prepares it for the specifics of the request.

Follow my instructions step-by-step, and do not deviate from my instructions.

Context: % add context %

Task:

- 1. Ask me what text I need editing. Wait for my reply. Do not continue until I reply.
- 2. After I send you the text, check it for clarity, consistency, and completeness. Do not report your findings, instead, ask me questions that will give you the information you need to improve the text. Consider the context described above between %%. Wait for my reply to your questions. Do not continue until I reply.
- 3. Based on my input, adjust the text to be clear, consistent, and complete. Highlight the changes you made by making the changed text bold. Do not make any other changes to the text. Show me the adjusted text. Wait for my reply.
- 4. Review the adjusted text. Pay attention to the following:
 - 4.1. Poorly structured sentences and suboptimal word choices.
 - 4.2. Consistency with the desired tone. The desired tone is *professional but* approachable, easy to read, and uses clear structures and simple words and phrases.
 - 4.3. Spelling and grammar.
- 5. Do not rewrite the text. Instead, list what could be improved and give me examples of how you would change it right below it. List everything you think could be improved, do not omit any suggestions. Number the elements on the list.

Logical Order & Segmentation

Arrange the details and instructions in a logical sequence. For example, if there are multiple steps to be followed, they should be presented in the order they need to be executed.

Break down the prompt into segments or paragraphs, each addressing a specific aspect of the prompt. This can include background information, the main question or task, and any specific requirements or criteria.



Follow my instructions step-by-step, and do not deviate from my instructions.

Context: % add context %

Task:

- 1. Ask me what text I need editing. Wait for my reply. Do not continue until I reply.
- 2. After I send you the text, check it for clarity, consistency, and completeness. Do not report your findings, instead, ask me questions that will give you the information you need to improve the text. Consider the context described above between %%. Wait for my reply to your questions. Do not continue until I reply.
- 3. Based on my input, adjust the text to be clear, consistent, and complete. Highlight the changes you made by making the changed text bold. Do not make any other changes to the text. Show me the adjusted text. Wait for my reply.
- 4. Review the adjusted text. Pay attention to the following:
 - 4.1. Poorly structured sentences and suboptimal word choices.
 - 4.2. Consistency with the desired tone. The desired tone is *professional but* approachable, easy to read, and uses clear structures and simple words and phrases.
 - 4.3. Spelling and grammar.
- 5. Do not rewrite the text. Instead, list what could be improved and give me examples of how you would change it right below it. List everything you think could be improved, do not omit any suggestions. Number the elements on the list.

Clear Instructions

The instructions must be unambiguous and specific!

The instruction should refer to the context.

Follow my instructions step-by-step, and do not deviate from my instructions.

Context: % add context %

Task:

- 1. Ask me what text I need editing. Wait for my reply. Do not continue until I reply.
- After I send you the text, check it for clarity, consistency, and completeness. Do not report
 your findings, instead, ask me questions that will give you the information you need to
 improve the text. Consider the context described above between %%. Wait for my reply to
 your questions. Do not continue until I reply.
- 3. Based on my input, adjust the text to be clear, consistent, and complete. Highlight the changes you made by making the changed text bold. Do not make any other changes to the text. Show me the adjusted text. Wait for my reply.
- 4. Review the adjusted text. Pay attention to the following:
 - 4.1. Poorly structured sentences and suboptimal word choices.
 - 4.2. Consistency with the desired tone. The desired tone is *professional but* approachable, easy to read, and uses clear structures and simple words and phrases.
 - 4.3. Spelling and grammar.
- 5. Do not rewrite the text. Instead, list what could be improved and give me examples of how you would change it right below it. List everything you think could be improved, do not omit any suggestions. Number the elements on the list.

Delimiters

Delimiters are used to separate and organize information. They help in defining the beginning and end of sections, grouping similar elements, or imposing output format.

Thanks to delimiters an AI model can "see" which part of text we refer to.



Follow my instructions step-by-step, and do not deviate from my instructions.

Context: % add context %

Task:

- 1. Ask me what text I need editing. Wait for my reply. Do not continue until I reply.
- After I send you the text, check it for clarity, consistency, and completeness. Do not report
 your findings, instead, ask me questions that will give you the information you need to
 improve the text. Consider the context described above between %%. Wait for my reply to
 your questions. Do not continue until I reply.
- Based on my input, adjust the text to be clear, consistent, and complete. Highlight the
 changes you made by making the changed text bold. Do not make any other changes to the
 text. Show me the adjusted text. Wait for my reply.
- 4. Review the adjusted text. Pay attention to the following:
 - 4.1. Poorly structured sentences and suboptimal word choices.
 - 4.2. Consistency with the desired tone. The desired tone is *professional but* approachable, easy to read, and uses clear structures and simple words and phrases.
 - 4.3. Spelling and grammar.
- Do not rewrite the text. Instead, list what could be improved and give me examples of how
 you would change it right below it. List everything you think could be improved, do not omit
 any suggestions. Number the elements on the list.

Format

Specify the format of the output. Describe how the response to your prompt should look like – should it be a written paragraph or bullet points, should it be detailed or concise, etc.

Use delimiters to establish a predefined structure for the output.

Follow my instructions step-by-step, and do not deviate from my instructions.

Context: % add context %

Task:

- Ask me what text I need editing. Wait for my reply. Do not continue until I reply.
- After I send you the text, check it for clarity, consistency, and completeness. Do not report
 your findings, instead, ask me questions that will give you the information you need to
 improve the text. Consider the context described above between %%. Wait for my reply to
 your questions. Do not continue until I reply.
- 3. Based on my input, adjust the text to be clear, consistent, and complete. Highlight the changes you made by making the changed text bold. Do not make any other changes to the text. Show me the adjusted text. Wait for my reply.
- 4. Review the adjusted text. Pay attention to the following:
 - 4.1. Poorly structured sentences and suboptimal word choices.
 - 4.2. Consistency with the desired tone. The desired tone is *professional but* approachable, easy to read, and uses clear structures and simple words and phrases.
 - 4.3. Spelling and grammar.
- 5. Do not rewrite the text. Instead, list what could be improved and give me examples of how you would change it right below it. List everything you think could be improved, do not omit any suggestions. Number the elements on the list.

Constraints

Instruct the model what it must and cannot do.

"Wait for my reply" will be commonly used in iterative prompts. If the AI must gather input from you before proceeding, you must very clearly state that you expect it to wait for your response.

Here, we added "do not proceed before I reply" because we ask the model to wait multiple times and we want to be extra specific that it is to wait with the next step until we respond.

Activity

Use the prompt to improve a piece of text. Experiment with what happens when you change the desired tone.



Activity

Exercise text (if you do not have your own)



https://docs.google.com/document/d/1L-vwdU9i9S2DBR2Ui0h5Ta8rcS9A6nGL_-dcU3uKo2k/edit?usp=sharing



Activity

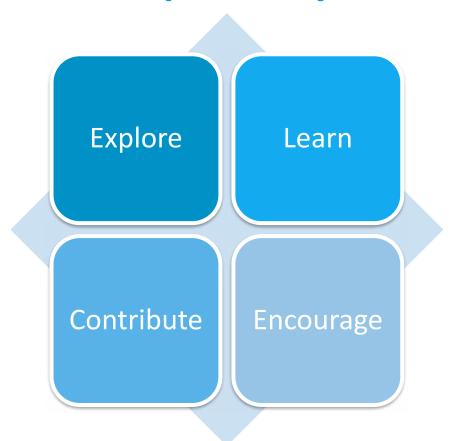
Example solution



https://chatgpt.com/share/66fe9681-3b58-8005-8de1-6a2373ae0538



How to use the Prompt Library?





Bonus!

What is gene Why does prom

The AI prompt engineering skills module

are out there? ct you privacy?

How to prompt effectively, and use the Prompt Library?

Feedback request

- New module on prompting -> https://umlib.nl/prompting
- Builds on information from generative Al module

- Teach students
 - level of understanding of prompting
 - Framework to build reliable prompts





How to provide feedback

- Wooclap questionnaire
 Scan the QR-code or email Noah
 Pecasse
 noah.pecasse@maastrichtuniversity.nl
- Or email your feedback directly to Noah Pecasse
- https://umlib.nl/prompting



The end...

What is gen are out there? ct you privacy? Why does prom Closure How to prompt effectively, and use the Prompt Library?



Important

Community of Practice: <u>UM-AI & Education: Community of Practice |</u>
 General | Microsoft Teams

• Edlab website: <u>Large Language Models and education - This is us! -</u>
Maastricht University



Lunchbreak

Back at 13:45 for panel discussion

