Prompt Engineering & AI Safety — Simple and Practical Guide

Introduction

Prompt engineering, the practice of crafting effective instructions for artificial intelligence (AI) systems, has become critical as AI tools like ChatGPT, DALL-E, and others are increasingly used in education, business, and creative fields. Effective prompt engineering enables users to get precise, safe, and useful outputs from AI, while also minimizing risks related to privacy, security, and ethical concerns. For high school students, office teams, or anyone new to AI, understanding how to design good prompts and use AI systems safely is essential for harnessing the technology's benefits and avoiding common pitfalls.

This report provides a practical guide to prompt engineering and AI safety. It explains what a prompt is, why prompts matter, the structure of a good prompt, and gives many examples of good and bad prompts. It also offers prompt templates for office teams, discusses safety rules, and outlines what information should never be uploaded. Finally, it addresses strategies to avoid AI mistakes, all in accessible language with clear examples.

What Is a Prompt?

A prompt is a set of instructions or a question you give to an AI system to get a specific response. In simple terms, it is the message you type into a chatbot or AI writing tool that tells the AI what you want it to do. For example, if you use an AI chatbot and type, "Write a summary of World War II in 100 words," your message is the prompt.

In AI systems, especially those that use natural language, prompts guide how the AI interprets your request and what kind of answer it provides. Just like you would ask a friend or a teacher a clear question to get a helpful answer, you need to be clear and specific when talking to AI.

Why Prompts Matter

Prompts are important because they directly affect the quality, accuracy, and safety of the AI's response. A good prompt helps the AI understand your needs, leading to relevant and reliable results. On the other hand, a vague or confusing prompt can produce off-topic, misleading, or even unsafe answers.

For example, in an educational context, students who learn how to write clear prompts can use AI tools to support their learning, improve their projects, and gain a better understanding of complex topics (Chowdhury,

2025; Siddharth et al., 2025). In office environments, clear prompts can help teams automate tasks, draft documents, or analyze data more efficiently. However, poorly written prompts can result in confusion, wasted time, or even privacy risks if sensitive information is accidentally shared (Weichert & Eldardiry, 2025).

Structure of a Good Prompt

A well-structured prompt usually has the following characteristics:

1. **Clarity**: The prompt is easy to understand and leaves no room for confusion.
2. **Specificity**: The prompt includes enough detail about what is required.
3. **Context**: The prompt provides background or sets the situation, if needed.
4. **Constraints**: The prompt may include limits, such as word count, style, or format.
5. **Purpose**: The prompt explains why the information is needed or how it will be used.

Example of a Good Prompt Structure

Suppose you want an AI to help you write a summary for your class project:

- **Bad Prompt**: "Tell me about climate change."
- **Good Prompt**: "Write a 150-word summary explaining the main causes and effects of climate change for a high school science project. Use simple language."

The good prompt is clear, specific about length, provides context (school project), and sets a style (simple language).

Examples of Good & Bad Prompts

Below are several examples showing the difference between effective and ineffective prompts across various scenarios.

Educational Examples

- **Bad Prompt**: "Explain photosynthesis."
- **Good Prompt**: "Explain the process of photosynthesis in plants in less than 100 words, suitable for a ninth-grade biology student."
- **Bad Prompt**: "Write an essay."

- **Good Prompt**: “Write a 200-word essay discussing the impact of artificial intelligence on society, including at least two positive effects and one challenge.”

Creative Writing Examples

- **Bad Prompt**: “Write a story.”
- **Good Prompt**: “Write a short story (200 words) about a student who invents a helpful robot to solve a problem at school. Use a lighthearted tone.”

Office Team Examples

- **Bad Prompt**: “Make a report.”
- **Good Prompt**: “Create a one-page summary of last month’s sales data for the marketing team, highlighting the top three products and any major trends.”

Safety & Ethical Examples

- **Bad Prompt**: “Give me a list of people’s email addresses.”
- **Good Prompt**: (This is actually not appropriate—see safety section.)

AI Mistake Examples

- **Bad Prompt**: “Can you give medical advice for my symptoms?”
- **Good Prompt**: “Provide general information on cold and flu symptoms, but do not offer medical advice. Remind me to consult a healthcare professional.”

These examples show that good prompts are clear, detailed, and avoid asking for sensitive, private, or dangerous information.

Prompt Templates for Office Teams

Office teams can use prompt templates to standardize requests and improve productivity. Here are some practical templates:

1. **Meeting Summary**
   “Summarize the main points and action items from the following meeting notes: [Paste meeting notes here].”
2. **Email Draft**
   “Draft a professional email to [Name or Department] about [subject]. Include a polite introduction, the main message, and a closing statement.”

3. **Project Update**
   "Create a brief project update for stakeholders, including current status, recent achievements, and next steps. Use a formal tone."
4. **Data Analysis Request**
   "Analyze the following data set for trends and outliers. Provide a summary in bullet points: [Paste data]."
5. **Checklist Creation**
   "Generate a checklist for launching a new product, including tasks for marketing, sales, and customer support."

Using templates like these helps ensure team members receive consistent, high-quality outputs from AI tools.

Safety Rules: Privacy, Security, and Responsible Use

AI safety is crucial, especially when using online tools that process personal or sensitive data. Understanding what to share and what to keep private protects both individuals and organizations.

What Information Should Never Be Uploaded

Never upload or include the following in AI prompts:

- Personal identification numbers (like Social Security, passport, or ID numbers)
- Financial information (credit card numbers, bank details)
- Passwords or login credentials
- Private health information
- Confidential business data (trade secrets, internal reports)
- Personal contact details (home addresses, private phone numbers, email lists)
- Student records or grades
- Any information protected by privacy laws (such as FERPA, HIPAA, GDPR)

Example of Unsafe Prompt:
"Analyze this list of employee names, emails, and salaries for trends." (Never upload such data to public AI services.)

Safer Approach:
"Analyze this anonymized sales data for trends. No personal or confidential information included."

Security and Privacy Best Practices

- **Use Official Accounts**: Always use company-provided or school-verified accounts when working with sensitive information.
- **Anonymize Data**: Remove names, addresses, or other identifiers before uploading.
- **Check AI Service Policies**: Understand how the AI tool stores and uses your data.
- **Restrict Access**: Only allow authorized team members to use the AI tool for official tasks.
- **Educate Team Members**: Regularly train staff on privacy and security risks (Weichert & Eldardiry, 2025).

How to Avoid AI Mistakes

AI systems are powerful but not perfect. They can make mistakes, misunderstand your requests, or generate biased or unsafe outputs. Here are strategies to avoid common pitfalls:

1. Review Outputs Carefully

Never assume the AI's answer is always correct. Double-check facts, especially for important decisions or public documents (Chowdhury, 2025).

Example:
If the AI writes a summary of a scientific article, read the original article to confirm accuracy.

2. Avoid Sensitive Topics

Do not ask AI systems for medical, legal, or financial advice. AI is not a substitute for professionals.

Example:
Instead of "What medicine should I take for these symptoms?"
Ask: "What are common cold symptoms? Remind me to consult a doctor."

3. State Your Needs Clearly

Be specific about what you want. If you get an unexpected answer, refine your prompt and try again.

Example:
If the AI gives a summary that is too long, update your prompt: "Summarize in under 100 words."

4. Use Neutral and Inclusive Language

AI can sometimes reflect biases present in its training data. Avoid prompting AI in ways that might reinforce stereotypes.

Example:
Instead of "Describe a typical engineer," try "Describe the key skills and education needed for an engineer."

5. Avoid Re-uploading Data

Don't repeatedly upload the same sensitive data. Each upload increases the risk of accidental exposure.

6. Stay Updated on AI Policies

Keep informed about updates to AI tools and organizational policies. Participate in training sessions and review guidelines regularly (Feffer et al., 2023).

7. Report and Learn from Mistakes

If you notice the AI makes a mistake or generates harmful output, report it to your teacher, supervisor, or IT department. Learn from incidents to improve future use.

Case Study: AI Safety in Education

A recent classroom study showed that when students interacted with real-world examples of AI mistakes (such as privacy breaches or biased outcomes), their awareness of AI risks increased significantly (Feffer et al., 2023). By using databases of past AI incidents, students learned to anticipate possible harms and became more cautious in their use of AI tools.

This approach highlights the importance of integrating AI safety education into school and workplace training. Students and staff who understand both the benefits and risks of AI are better equipped to use these technologies responsibly (Siddharth et al., 2025; Chowdhury, 2025).

Conclusion

Prompt engineering is a foundational skill for anyone using AI systems in school, the workplace, or creative projects. Writing clear, specific prompts yields better results, saves time, and reduces misunderstandings. However, with great power comes responsibility: users must be careful not to share private information or request unsafe outputs. By following the practical

advice in this guide—structuring prompts thoughtfully, using templates, applying safety rules, and regularly reviewing AI outputs—students and office teams can use AI tools safely and effectively.

Ongoing education about AI risks, ethics, and responsible use is essential. As AI becomes more integrated into daily life, everyone must develop both technical skills and a sense of responsibility to ensure AI serves as a positive force for learning, creativity, and productivity.

References

Chowdhury, T. (2025). Computational Thinking with Computer Vision: Developing AI Competency in an Introductory Computer Science Course. Retrieved from https://arxiv.org/pdf/2503.19006v1

Feffer, M., Martelaro, N., & Heidari, H. (2023). The AI Incident Database as an Educational Tool to Raise Awareness of AI Harms: A Classroom Exploration of Efficacy, Limitations, & Future Improvements. Retrieved from https://arxiv.org/pdf/2310.06269v1

Siddharth, S., Prince, B., Harsh, A., & Ramachandran, S. (2025). The World of AI: A Novel Approach to AI Literacy for First-year Engineering Students. Retrieved from https://arxiv.org/pdf/2506.08041v1

Weichert, J., & Eldardiry, H. (2025). Educating a Responsible AI Workforce: Piloting a Curricular Module on AI Policy in a Graduate Machine Learning Course. Retrieved from https://arxiv.org/pdf/2502.07931v1