Guidelines for Elementary, Junior High and Senior High School Students on Using Generative Artificial Intelligence

Approved by the Ministry of Education, Republic of China, on July 1, 2024
(Taiwan Education Resource (3) Letter No. 1132702614)

In recent years, the rapid development of generative artificial intelligence (generative AI) and deepfake technologies has resulted in numerous opportunities and changes for society. These technologies have transformed the ways we acquire knowledge, disseminate information, and create content. However, the risks associated with their use have also increased. To improve student literacy in using generative AI tools, to assist students in skillfully using these technologies, and to prevent misuse or abuse, the following four guidelines are provided for reference.

1. Potential for Biased Content

Generative AI tools are based on historical records or experiences. If these sources contain biases or errors, the output of generative AI tools may also be biased or incorrect, because these tools cannot independently verify the accuracy or reasonableness of their results.

Therefore, we must carefully examine the content generated by generative AI tools whenever we use them.

2. Reduction in Information Diversity

The data used by generative AI tools are influenced by their sources. If the data are not diverse or extensive, the output may only reflect knowledge from a single culture, leading to a substantial lack of accuracy and potentially fostering bias.

Therefore, instead of just accepting the generated content as it is, we must examine the content based on our own experience and critical thinking skills whenever we use generative AI tools.

3. Risks of Deepfake Technology

Deepfake is modifying face portrait technology, which uses generative AI to create fake content, and can be used to manipulate images, videos, or audio materials to produce realistic content, including fake news.

Hence, when viewing online content, we must not readily trust unverified videos or photographs and must be aware of the possibility that this content may have been synthesized using deepfake technology. We must also assess the motives and intentions behind the creation of such content.

4. Privacy and Confidentiality Risks

Some generative AI tools lack comprehensive legal, regulatory, and ethical oversight concerning the acquisition, storage, and use of data. Therefore, the personal information, sensitive messages, and confidential data provided when using these tools may be incorporated into training databases and used in future responses to others.

When using generative AI tools, we must strictly and carefully assess the provided information for any content related to confidentiality, privacy, or sensitivity. In this way, we protect the privacy and confidentiality of individuals and organizations.
Although generative AI has resulted in substantial convenience for our lives and has been widely applied in various contexts, it still carries risks and challenges. In this digital age, we must:

(1) Maintain a high level of vigilance regarding information sources.

(2) Avoid easily believing unverified information.

(3) Learn to identify false information.

Meanwhile, we must improve our critical thinking abilities.

(1) We must critically analyze and evaluate the content created by generative AI tools to avoid being misled.

(2) We must adhere to ethical and legal standards (e.g. respecting intellectual property rights) to ensure that the use of generative AI tools does not violate social norms and information ethics.

Finally, we must strengthen our digital literacy. Only by strengthening digital literacy can we enjoy the considerable convenience of technological advancements, minimize the risks, and reduce the negative effects of generative AI.

Appendix

Guidelines for Elementary, Junior High and Senior High School Students on Using Generative Artificial Intelligence

PARADIGMS

1. Potential for Biased Content. When we ask a generative AI tool to suggest a travel itinerary, if the system's database lacks the correct information about local climate, geographical locations, social customs, and cultural restrictions, the provided content may be a mere synthesis of various online travel blogs. This can result in an itinerary which is out of your way, out-of-season, or even includes nonexistent attractions.

2. Reduction in Information Diversity. When we consult a generative AI tool for legal or cultural inquiries, the answers may be based on the laws and cultural practices of the developer's country. Similarly, if we request a generative AI tool to generate an image of a bride, it may produce an image of a Western woman in a white gown, rather than reflecting the diverse cultural customs of the user's locale, such as varied skin tones or wedding attire.

3. Discovering that Deepfake Technology can Generate False Content. Numerous online videos involve well-known individuals giving speeches or encouraging investments. When encountering such content, we must carefully verify the information and its sources. In the rapidly evolving online environment, deepfake technology may integrate the faces and voices of these individuals into entirely false and defamatory videos without their consent or knowledge.

4. Potentially Causing the Leakage of Personal Data, Privacy, and Confidential Information. When we ask generative AI tools questions containing personal or academic information, without fully understanding the principles and regulations that govern the operations of these tools, then we risk incorporating our personal or academic information into the training databases of these tools. When other users subsequently ask similar questions, then the generative AI tool can respond with information from the stored database, which could lead to breaches of confidential, personal or academic information, and therefore security vulnerabilities.