
Safe use of AI tools

Recommendations from Charles University's management for the safe use of AI tools



The management of Charles University would like to make the academic community aware of security threats that have been identified in some generative artificial intelligence tools. In this context, we do not recommend the implementation and use of DeepSeek for work and academic purposes.

We recommend that you follow the recommendations of the National Cyber and Information Security Agency (NÚKIB) when using applications for generative AI and other services as well, especially those that are free of charge and freely accessible. For more information see (only in Czech language):

[The National Cyber and Information Security Agency – NÚKIB recommends caution when using trendy or popular apps](#) .

Although the National Cyber and Information Security Agency has not yet commented directly on the use of DeepSeek, we recommend that the entire academic community avoid using it for their work and study tasks.

Extreme caution should also be used with other chatbots from Chinese manufacturers, such as Qwen from Alibaba. The use of tools developed and administered by entities under the jurisdiction of countries with restricted academic freedom may pose an institutional risk leading to potential illegitimate influence on academic activities.

The personal data of registered users of the system is at risk, as evidenced by the reserved approach and caution expressed by Member States at the last meeting of the European Data Protection Board on 11 February 2025. The DeepSeek tool should be thoroughly reviewed and monitored on the European AI platform. The misuse of documents and inputs, including login data, cannot be ruled out, and the intellectual work of researchers and students is also at risk.

We recommend using tools that are protected against security risks on a contractual and technical basis. For the widest use at the university, Microsoft Copilot for Education is a suitable tool and is available to all employees and students of Charles University on their web browser: [Microsoft Copilot for Education](#) .

For advanced use, we recommend a Microsoft 365 Copilot employee licence, which is integrated into online applications (e.g. Excel, Word, Outlook,).

A regularly updated list of recommended and verified tools is available [here](#)

If you intend to use another tool for your work, research, or studies and are not sure how safe it is, please contact the AI team at the E-Learning Support Centre – elarning@cuni.cz.

The management of Charles University invites experts in the field of generative AI to collaborate on expanding this list of resources and also to participate in the [Working Group for Generative AI at CU](#).

Charles University welcomes all educational activities that are organized by the Rectorate, faculties, and research teams and that focus on the safe and practical use of generative AI tools. We have been gradually collecting information about these tools on the web page <https://ai.cuni.cz> and have been informing the university about them in a [special newsletter](#) . For introducing employees to the principles of working with generative AI tools, we recommend taking the e-course prepared by the Faculty of Humanities: [Introduction to Generative AI](#) (only in Czech language)) or the free online courses that are prepared in many language versions, including English, Czech and Ukrainian, [Elements of AI](#) .

