ITEC

European Parliament

Guidelines

Use of publicly available

Artificial Intelligence tools for Parliament staff

Version: 16 April 2024

Purpose of this document

The emergence of a new generation of Artificial Intelligence (AI) tools, rooted in generative AI models, is reshaping work dynamics and societal norms. Generative AI (also known as gen-AI) models are sophisticated computer programs crafted to produce new content that closely resembles human-created output. These models are accessible to anyone through online chatbots, allowing users to request tasks, such as drafting or summarising text, generating unique images, or suggesting visual representations for spreadsheet data. Some examples of such tools are: ChatGPT, Dall-E, Midjourney, Gemini, LaMDA, Aleph Alpha, Bloom, and Stable Diffusion.

The guidelines aim at supporting staff working in the European Parliament[1] on the safe use of publicly available generative AI.

The guidelines apply only to third-party publicly available generative AI tools. AI-enabled tools that are either developed or acquired internally by the European Parliament are outside of the scope and are assessed on a case-by-case basis in line with the current IT policy and standard frameworks that have been established in the European Parliament[2].

Staff can make use of generative AI tools under the strict understanding that these tools should only support them in the course of performing their professional duties and shall not replace the work of a staff member (see Information sheet 1). In other words, AI tools are merely tools: staff remains responsible for the execution and the quality of the tasks they perform.

Staff should always be vigilant when it comes to inherent risks and limitations (see Information sheet 2).

[1] Statutory staff (officials, temporary agents and contract agents), seconded national experts and contractors or other service providers.
[2] In particular, policies and standards regarding the domains of cloud technologies, information security, data protection and risk management.

Principles

Principle n°1: Non-Disclosure and personal data protection

Parliament staff must never share any European Parliament information that is not already in the public domain with publicly available generative AI tools.

Parliament staff must never share any personal data with such tools, even if this personal data is already publicly available.

Parliament's staff is reminded of Article 17 of the Staff Regulations[3] which forbids the unauthorised disclosure of any information received in the line of duty unless that information has already been made public, or is accessible to the public, even after leaving the service (see also Article 339 TFEU). Staff must be aware that any input provided to an online generative AI tool is transmitted to the provider who can use this information to generate future outputs, subsequently disclosing the information to the public at large.

Similarly, external contractors are bound by the non-disclosure of information clauses in their contracts.

Staff is reminded of the obligation to comply with Regulation (EU) 2018/1725 when the processing of personal data is involved, even if the data is already publicly available. Sharing personal data with such tools constitutes processing of personal data running the risk of this data being further processed by the provider of the AI tool for other purposes over which the Parliament has no control. As a consequence, feeding AI tools with personal data for which the EP is responsible would generate a risk of non-compliance with Regulation (EU) 2018/1725.

Principle n°2: Content responsibility

Parliament staff should not directly replicate generative AI results. They remain always responsible for any material they produce.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01962R0031-20140501,

Parliament staff must ensure that there is a thorough human review, either individual or collective, of any output based on AI inputs before it is used in their work.

Although the performance of generative AI tools is constantly improving, staff must be aware that they can produce biased and wrong answers to a user prompt. AI generated content can be innaccurate, unethical, misleading and even partially or entirely fabricated, as "hallucinations"[4] from the AI algorithm can occur. It is therefore crucial that Parliament's staff reviews and confirms the validity of the output.

In the case of collaborative work, discussion and agreement among colleagues must ensure human quality control over the information generated via AI tools.

Principle n°3: Transparency and Compliance

Parliament staff must always properly reference sources when making substantial[5] use of generative AI tools, using the disclaimer "AI-assisted".

Likewise, staff should always critically assess whether or not the outputs of an online publicly available generative AI model are violating intellectual property rights, in particular copyright infringements of third parties. In case of doubt or where such assessment cannot be carried out, staff must refrain from using such outputs[6].

Lack of transparency on the origin of materials used for training generative AI models raises concerns related to intellectual property rights, in particular copyright. Copyrighted information could end up reproduced verbatim (or almost verbatim) in replies to a user prompt, without any credit or reference to the source or the author. The same applies to images, videos and graphic content.

[4] An "*AI hallucination"* is when a generative AI model generates inaccurate information as if it were correct, e.g. making up laws and cases which do not exist.
[5] For example, using generative AI as a basic author support tool is not a substantial use. However, interpreting data analysis, generating draft legislation, developing hypotheses, etc. could have a substantial impact.
[6] Once established, the AI act foresees that the EU AI office will monitor the compliance of AI providers with the EU copyright law. Users will be informed regularly on the list of third-party providers that comply with such EU copyright law.

Principle n°4: Autonomy and Business Continuity

Parliament staff should never rely exclusively on online publicly available generative AI models for mission-critical and time-sensitive processes.

Publicly available generative AI models are known to show stability problems, such as long response times or unavailability of the service. There are typically no promises made on availability. In case of tight deadlines or when Members, other colleagues or services are depending on a deliverable to perform their duties, relying exclusively on such tools bears a risk of business continuity.

Guidelines lifecycle and support

As the technology of publicly available generative AI tools evolves, so do the related advantages, risks, limitations, and legal provisions. Therefore, this document will be updated as required.

The publication of the guidelines and their evolution will be supported by awareness raising activities.

Parliament's IT services are responsible for the guidelines lifecycle and the support. Should staff identify any new or different risks in the usage of public AI tools, or in case of doubt on usage situations, please refer to AI-EP@europarl.europa.eu. These risks will be assessed and the relevant follow-up instigated.

Information sheet 1

Practical examples

To support a safe use of third-party publicly available generative AI tools, here are some practical examples of possible and prohibited usage.

Possible usage while respecting the principles

- Help generate rough draft texts, such as reports, news articles, social media publications or webpages on the basis of publicly available information (excluding personal data).
- Help generate rough translations or summaries of publicly available texts such as information leaflets or public texts.
- Help generate suggestions for rephrasing or formulating more interesting text snippets, or correcting grammar of public texts.
- Help analyse or answer questions on publicly available data.
- Help generate suggestions for software code.
- Help generate image proposals.

Examples of usage to be avoided

- Inputting non-public information, such as working documents of the European Parliament.
- Inputting personal data, such as for the generation of evaluation reports.
- Copying, quoting, replicating or publishing the outputs from generative AI tools as EP produced content, without thorough human control and the disclaimer “AI-assisted”.
- Use software code generated by AI without human review. This is to ensure that unsecure or even malicious code is not introduced into the European Parliament IT systems.
- Seeking legal or administrative advice.

Information sheet 2

Frequently asked questions

While it is important to explore the potential benefits of publicly available generative AI models for professional purposes, it is equally important to be aware of the associated risks. Like any other information and communication tool used by staff in the European Parliament, online generative AI models should only be used when appropriate and safe.

What is “Generative Artificial Intelligence”?

The emergence of a new generation of AI tools, rooted in generative AI models, is reshaping work dynamics and societal norms. Generative AI models are sophisticated computer programs crafted to produce new content that closely resembles human-created output. These models are accessible to anyone through online chatbots, allowing users to request tasks, such as drafting or summarising text, generating unique images, or suggesting visual representations for spreadsheet data.

How does it work?

The model works by learning patterns and characteristics from a large collection of data. When a user prompts the model, for example with a question or with an image, it generates a response that statistically aligns with its previous learning. It could assist colleagues to write briefings, produce policy summaries, develop computer code for new software, anticipate answers to audit questions or summarise surveys, to mention just a few examples.

Which are publicly available “Gen-AI tools”?

Among the most prominent tools currently available are ChatGPT, Dall-E, Midjourney, Gemini, LaMDA, Aleph Alpha, Bloom, and Stable Diffusion.

What is the most prominent risk in using such tools?

The most prominent risk is the unauthorised disclosure of information received in the context of one’s work. Any input provided to an online generative AI chatbot is transferred to the provider of the chatbot, which can subsequently use this information to generate future outputs that could be disclosed to the public at large.

Staff working at the European Parliament could inadvertently disclose information that is categorised as not for public disclosure, as defined in the Information Security Policy of the

European Parliament[7], or data that is classified as “personal” within the meaning of EU Data Protection Regulation[8] article 3(1) or subject to copyright. Examples of such personal data could be: sensitive characterists revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person’s sex life or sexual orientation or criminal convictions.

Are “Gen-AI” tools trustworthy?

The fact that there is little transparency on which datasets are being used to train these publicly available models, the programming techniques employed or how decisions within the model are achieved, leads to a potential ‘black box’ effect, with ethical and reputational implications regarding the trustworthiness of the results.

It is currently not possible for generative AI models to properly list and credit the materials it is reproducing in its output, making it difficult to obtain the necessary authorisation from the copyrights owners, while the tools owners often waive any responsibility in this regard.

Are “Gen-AI” tools reliable?

The current AI tools are far from flawless. They may yield outcomes that at first seem comprehensive, but which at a closer look exhibit bias, lack completeness, or are simply erroneous. This in turn could generate the risk of misinterpretation by creating or spreading information that can be misleading or that misrepresents the European Parliament.

The creators of generative AI models are not always transparent on the data and algorithms used. Hence, it is difficult to assess the reliability of an answer generated by such a model. Moreover, the models are not updated in real time and typically do not take into account the most recent data.

Likewise, ill-intentioned actors can take advantage of the situation and create fake AI tools, disguised as popular AI models, in order to collect personal and business data for malicious purposes. It is therefore important to verify the generative AI model’s sources.

[7] See Information security policy in the European Parliament (https://epintranet.in.ep.europa.eu/files/live/sites/epintranet/files/finance/reporting-discharge/info-security-policy-ep.pdf)
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725