

APPROVED  
By Decision No. 3 of the Minutes No. 04/2026  
of the NDAL Senate meeting of 18 May 2026  
In effect as of 2 June 2026  
by Order No. 51 of the Rector of NDAL

## **Terms of Use of Artificial Intelligence at the National Defense Academy of Latvia**

### **I. General provisions**

1. The Terms of Use of Artificial Intelligence (hereinafter – AI) provide an explanation of the basic principles of the correct use of AI, compliance with these terms and the procedure for reviewing violations at the National Defence Academy of Latvia (hereinafter – NDAL).

2. The administration of NDAL, students, unenrolled attendees, academic, administrative staff and other persons who participate and cooperate in the educational process at NDAL have an obligation to comply with the rules for the use of AI at NDAL, as well as AI usage guidelines with classification levels and clarifications of permitted/to-be-performed actions (see Annex 1), prevent violations and inform about them.

### **II. Terminology**

3. Artificial intelligence – a machine-based system that is designed to operate with varying levels of autonomy, can be adaptive, and is capable of, according to explicit (expressed) or implicit (accepted) goals, generating products from information entered into the system, such as predictions, text content, recommendations, and decisions that can affect the physical or virtual environment.

4. AI machine-based system – designed to perform narrow procedural tasks, to improve the outcome of previously completed human activity, but it is not intended to replace or influence previously completed human assessment without human supervision.

5. Widely used machine learning systems – AI tools (e.g. *Chat GPT, Microsoft Copilot, Bard, Bing, Claude*) that can be used to obtain explanations of concepts, generate new ideas, improve text quality, and gain a general idea of large amounts of material, as an assistant for translating texts and as a “brainstorming” assistant when conducting independent research work.

6. Low-risk AI tools – machine-based systems that support the correction and verification of independently created works, as well as systems

that allow for the collection and processing of data, such as grammar correction, translation, audio-to-text transcription tools, and information search tools on the Internet.

7. High-risk AI tools – machine-based systems that can be accessed using AI tools (for example: *Chat GPT, Microsoft Copilot, Bard, Bing, Claude*), which are capable of generating autonomous products based on the information entered into the machine-based system.

8. Academic Integrity Commission – a commission established by order of the Rector of the NDAL to review cases of academic integrity violations, including non-compliance with the rules of NDAL.

9. CAPS – a plagiarism and text originality checking system used in the NDAL educational process which determines the percentage of AI in research work.

### **III. Compliance and promotion of integrity in use of AI**

10. NDAL supports and promotes modern approaches to the use of technology in the learning process, including various AI tools. Simultaneously, NDAL ensures that quality learning objectives are achieved and the principles of academic integrity are not violated. NDAL provides instructions and recommendations on the correct use of AI in the learning process to prevent and reduce the possibility of academic misconduct.

11. The academic and administrative staff of the NDAL and other persons who participate and cooperate in the educational process at the NDAL have a duty to promote the understanding of students and unenrolled attendees about the correct use of AI and the reduction of violations.

12. Measures for the correct use of AI in the NDAL:

12.1. when preparing an educational activity (e.g. a study course, an individual research assignment, a lecture, or a group work assignment), the lecturer or person conducting or responsible for the educational activity must clearly define the use of AI (whether the use of AI is permitted and, if permitted, to what extent);

12.2. students and unenrolled attendees may freely use low-risk AI tools when creating references, as these AI tools do not generate autonomous new content, except where the lecturer or person responsible for the educational activity has determined otherwise;

12.3. students and unenrolled attendees may use AI tools as sources of inspiration to improve the fluency of text, identify synonyms, expand literature reviews, translate and understand complex theories. In research work, AI-generated content must be cited like any other source and references must be

provided;

12.4. when using AI-generated products, students and unenrolled attendees shall indicate the developer of the AI tool (year of development), its name in the original language (version) (e.g. *Open AI. (2025). ChatGPT (January 25 version) [Large language model]*). <https://chat.openai.com/>).<https://chat.openai.com/>)

#### **IV. Restrictions on the use of artificial intelligence tools**

13. High-risk AI tools may not be used in individual assessments (tests, assessments, examinations), except where their use has been explicitly permitted by the lecturer or another person responsible for the educational activity. If a student or unenrolled attendee fails to comply with this provision, it shall be considered a case of academic fraud:

13.1. before using the selected high-risk AI tool, the student or unenrolled attendee must examine who developed the respective AI tool, what the developer does with the information it collects from the AI tool, and assess the risks it may pose to the user or third parties;

13.2. the student or unenrolled attendee must be able to distinguish their own intellectual contribution from the product generated by the AI tool, which cannot be considered to have been created by the author; likewise, the AI tool cannot be considered a co-author because an AI tool is not a person;

13.3. students and unenrolled attendees should avoid using a high-risk AI tool as their main or sole source of information, as the developed Internet search engines (low-risk AI tools) are specifically designed for this purpose and have a higher degree of reliability;

13.4. high-risk AI tools are not designed to perform mathematical calculations or data processing and therefore do not operate with the same accuracy as other tools specifically developed for these functions (e.g. calculators);

13.5. the student or unenrolled attendee must be aware that excessive use of high-risk AI when generating text may result in a research paper lacking the author's originality and intellectual contribution and, when such work is reviewed, a procedure similar to that applied in cases of plagiarism will be followed;

13.6. in accordance with the principles of academic integrity, NDAL ensures that all individual research papers are checked using the CAPS programme twice. For bachelor's, master's or qualification papers, this is ensured before the pre-defence of the paper (the first time) and before the defence of the paper (the second time). In other cases, a student or unenrolled attendee may approach the lecturer, the person responsible for the educational activity, or the research supervisor to have the paper checked using the CAPS programme; this activity is not regulated and is a collaborative process between the lecturer, the person responsible for the educational activity, the research

supervisor and the student/unenrolled attendee.

## **V. Types of academic integrity violations involving the use of artificial intelligence tools**

14. The following deliberate actions shall be considered academic integrity violations involving the use of AI tools:

14.1. use of high-risk AI tools where the lecturer or person responsible for the educational activity has explicitly prohibited their use;

14.2. use of high-risk AI tools without providing references in accordance with Clause 12.4 of these Terms;

14.3. unambiguous generation of text using high-risk AI tools, as indicated by CAPS (making it impossible to assess the author's intellectual contribution to the research work);

14.4. AI-generated text produced using high-risk AI tools exceeds 20% of the total volume of the research work.

## **VI. Review of violations and decision-making**

15. A person may be found guilty if they have been involved in an academic integrity violation – in writing, orally or in another form. If these Terms are not complied with, the violation shall be referred for consideration by a commission established by order of the Rector.

## **Guidelines for the Use of Artificial Intelligence (AI), with Classification Levels and Clarifications on Permitted/Required Actions**

### **1. General Principles**

All publicly available AI tools, including generative AI (e.g., chatbots, code generators, image and document generation platforms), are considered **untrusted**.

The Latvian National Armed Forces (NAF) have no ability to control, track, correct, or delete information entered into such tools, nor are there any guarantees regarding the security of data storage, the tool's security practices, or the model's future use.

### **2. Prohibited AI Tools**

All of the tools listed below are prohibited because they are developed, maintained, or provided in countries that are not considered safe for information processing. The use of these tools may pose risks of data leakage, tracking, and cyber threats.

- Chinese AI tools: DeepSeek, Baidu ERNIE Bot (Wenxin Yiyan), Alibaba Qwen / Tongyi Qianwen, Tencent Hunyuan AI, iFlytek SparkDesk, Zhipu AI / ChatGLM / GLM-4, ByteDance AI tools (including CapCut AI features, TikTok AI tools with data uploads), SenseTime SenseNova, Huawei Pangu AI, Kimi AI (Moonshot AI)

etc.;

- Russian AI tools: YandexGPT and Yandex generative AI services, SberGPT / SberDevices “GigaChat”, RuGPT-3 / RuGPT models, Tinkoff “TinkoffGPT”, VK / Mail.ru AI solutions (MARU, etc.), any AI tools or platforms hosted in Russian data centres;
- Belarusian AI tools: any tool managed or hosted in Belarus is prohibited, e.g., Synesis and related analytics/AI tools, GOV.BY digital AI services.

### **3. What Employees<sup>1</sup> May Do with Publicly Available AI Tools**

- write idea prototypes without data;
- request suggestions on publicly known topics;
- use AI for stylistic language improvement when the content is public;
- request assistance with developing concepts, provided that no organizational data is used;
- research industry trends and publicly available materials.

---

<sup>1</sup> In these guidelines, the term “employees” includes the NDAL management, academic and administrative staff, as well as students, listeners, and other persons insofar as they use AI tools within the NDAL.

#### 4. What Employees Are Strictly Prohibited from Doing

- entering any internal or restricted-access documents into an AI system;
- uploading files, screenshots, or photographs containing work-related information;
- entering personal data — even if it appears secondary or insignificant (GDPR violation);
- using AI to analyse or improve processes involving internal information;
- updating or generating documents classified within the organization as internal or restricted-access;
- using AI tools for decision-making that affects security, personal data, the SIS environment, financial and supply processes.

#### 5. Information Classification Levels and Permitted Actions

| Classification level | What may be done                                                                                                                                                                                                                                                | What is strictly prohibited                                                                                                                                                                                                                                                  |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Public information   | Generate ideas, texts, and structures;<br>Rephrase information that has already been published;<br>Request style or language improvements;<br>Create presentation frameworks;<br>Ask questions about publicly available topics.                                 | AI must not be provided with any internal organizational details that have not been publicly confirmed; AI must not be used to insert internal information into presentations at a later stage.                                                                              |
| Internal information | AI may be used only at a conceptual level, without providing any details;<br>Advice on process best practices may be requested without specific data;<br>Ideas may be tested if the text has been completely rewritten and the information is not identifiable. | Internal documents, protocols, or procedures must not be entered;<br>Examples containing the organization's operational context must not be included;<br>Files must not be uploaded or screenshots.                                                                          |
| Restricted access    | AI must not be used in any way related to the processing of this information;<br>The only permitted use of AI: general questions without content or context.                                                                                                    | Complete prohibition of uploading, copying, entering, or describing any restricted-access information in AI systems;<br>Editing, text improvement, or analysis using AI tools must not be performed;<br>Documents or policies must not be created with the assistance of AI. |

## 6. Specific Exception: Anonymized Data

Employees are permitted to use public AI tools to resolve technical problems or for certain data analysis only if the data entered are **fully anonymized and cannot be restored** (an anonymization algorithm must be developed and agreed upon with the Cybersecurity department):

- personal data;
- system configurations;
- security incident information;
- network structure;
- access rights;
- other classified information.

Anonymization means that the data are not merely replaced with other names, but are completely transformed so that it is impossible to de-anonymize them and identify the actual system or persons.

IT personnel are prohibited from:

- entering any log files containing IP addresses or system identifiers;
- entering configuration fragments that can be recognized by their structure;
- sending code fragments containing access methods, classified functions, or architectural structure;
- using AI to analyse a real incident or vulnerability.