University of Stuttgart
Germany

Policy on the Use of Artificial Intelligence (AI) and the Use of AI Systems at the University of Stuttgart

The Rectorate of the University of Stuttgart adopted the following Policy on the Use of Artificial Intelligence (AI) and the Use of AI Systems at the University of Stuttgart in its meeting on September 30, 2025.

Preamble

The use of Artificial Intelligence (AI) opens up new opportunities for the University of Stuttgart in terms of efficiency, quality improvement, and innovation. At the same time, the responsible use of AI systems requires certain legal, ethical, and organizational provisions.

This AI Policy is based on the understanding of a modern university that purposefully leverages technological opportunities while safeguarding the protection of individuals and their personal rights, maintaining the integrity of the organization, and continuously reflecting on its use of new technologies — in this case, AI systems.

In view of the rapid technological developments in the field of Artificial Intelligence and the evolving legal and societal frameworks, this policy will be reviewed and updated regularly. Its purpose is to provide all employees with a reliable framework for using AI systems at the University of Stuttgart in a secure, responsible, ethically sound, transparent, and legally compliant manner.

Scope: This policy applies to all employees of the University of Stuttgart who use AI systems as part of their professional duties outside of research, such as for project management, third-party funding administration, the organization of examinations, or committee work. It is complemented by the following documents:

- Levels of Confidentiality for Information in the Context of the Use of AI Systems
- Whitelist for the Different Types of AI Systems

The final decision on whether—and especially which—AI systems may be used for official purposes outside of research rests with the University Executive Board. For employees engaged in research, this policy also applies in addition to further specific regulations.

1. Definition of AI Systems and Relevance of Information Classification

AI systems, as defined in this policy, are software-based applications that use data- or rule-based methods to autonomously process or generate information and to support human decision-making or problem-solving processes.

This includes, in particular, systems that allow users to interact in dialogue form (e.g. via text input) and that generate output either in real time or asynchronously. Examples include chatbots (e.g. ChatGPT), writing assistants (e.g. Copilot, DeepL Write), image or analytics generators (e.g. Midjourney, AI-supported dashboards), as well as business intelligence systems that automatically classify data (e.g. Power BI).

Even the input of information into such systems—whether structured (e.g. tables, databases, Excel files) or unstructured (e.g. texts, images, audio, or video files)—is relevant for data protection and information security. This is because an AI system may not only store or process such information but may, in some cases, also use it for self-improvement (e.g. training future model versions). Therefore, when using any AI system, **it is crucial to assess what kind of information is entered**—not just what the system outputs.

This AI Policy is based on the levels of confidentiality for information in the context of AI system use, available as a separate document.

Before entering any information into an AI system, users must carefully determine which level of confidentiality the information applies to.

- If a classification already exists, it must be followed.
- If no classification exists, users are obliged to define the level of confidentiality themselves in due diligence or request classification from a higher authority (e.g. supervisor, Rectorate).

2. Principles of AI Use

- **AI systems are to be used as supporting tools.** They may support but must not replace human judgment or individual decision-making responsibility.
- **The protection of personal rights and confidential information takes highest priority.** Before using an AI system for professional purposes, users must verify which information may be entered into which system according to this policy. The processing of personal data requires a legal basis.
- **AI use must be as transparent as possible.** This means that functionality, decision logic, and responsibilities must be understandable for all affected persons.
- **Users are responsible for the quality and accuracy of any content that includes AI-generated results.** They must review AI-generated outputs carefully before use.

The university provides accessible information and training to ensure secure, responsible, ethical, and legally compliant AI use. It designates a central contact person for questions regarding AI use.

3. Types of AI Systems for Professional Use

This policy distinguishes the following types of AI systems, which define what data of which level of confidentiality may be entered:

- **Type 1 – University-owned AI systems:**
  AI systems fully operated by and within the University of Stuttgart, with no data transfer to external systems. These process data exclusively within university infrastructure and—after approval by the Rectorate—may be used for all confidentiality classes, including strictly confidential information (C4). Employees may enter C1–C4 data, however C3 and C4 data may only be entered after review and documented approval by their supervisor or higher authority.
- **Type 2 – University-operated AI systems using models hosted by scientific partners (e.g. GWDG):**
  AI systems operated by the university, accessing models hosted by trusted academic institutions such as GWDG (Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen). Employees may enter C1–C3 data, but C3 may only be entered after review and documented approval by a supervisor or higher authority.
- **Type 3 – University-operated AI systems using models from commercial providers (e.g. Azure OpenAI):**
  AI systems operated by the university that access models hosted externally in

EU cloud infrastructure. Employees may enter C1 and C2 data only. C3 and C4 data are not permitted.

- **Type 4 – External enterprise services with privacy-friendly settings and institutional contracts (e.g. ChatGPT Team):**
  Large provider systems accessible via university contracts and login with the university account, offering privacy-optimized settings. Employees may enter C1 and C2 data. C3 and C4 data are not permitted.
- **Type 5 – Public, unverified AI systems (e.g. ChatGPT Free):**
  Only C1 (public) data may be entered. C2–C4 data and any personal or confidential information must not be entered.

---

4. Permitted Use Cases

The following matrix defines which confidentiality classes may be used with which AI system types and under what conditions (e.g. after review). The specific use case (e.g. text drafting, planning, analysis with AI assistance) is permitted if the chosen combination of system type and confidentiality class allows it.

If the classification of a system is unclear, **only public (C1) data** may be entered.

	TYPE 1	**TYPE 2**	**TYPE 3**	**TYPE 4**	**TYPE 5**
Type of AI System/ Level of Confidentiality	**University-owned AI systems**	**University-operated AI systems using models hosted by scientific partners (e.g. GWDG)**	**University-operated AI systems using models from commercial providers (e.g. Azure OpenAI)**	**External enterprise services with privacy-friendly settings and institutional contracts (e.g. ChatGPT Team)**	**Public, unverified AI systems (e.g. ChatGPT Free)**
C1 – Public	✅ allowed	✅ allowed	✅ allowed	✅ allowed	✅ allowed
C2 – Internal	✅ allowed	✅ allowed	✅ allowed	✅ allowed	⛔ not allowed
C3 – Confidential	✅ allowed (after review)	✅ allowed (after review)	⛔ not allowed	⛔ not allowed	⛔ not allowed
C4 – Strictly confidential	✅ allowed (after review)	⛔ not allowed	⛔ not allowed	⛔ not allowed	⛔ not allowed

5. Transparency & Documentation

- If an AI system is used extensively—for instance, when drafting a text—this should be noted in the document (e.g. “Created with the help of GPT-4 on June 20, 2025”).
- If AI is used only minimally (e.g. for phrasing suggestions), no labeling is required.
- Labeling is mandatory when AI-generated content is directly reused in official publications, web pages, or external communications.
- If AI systems are used to respond to inquiries—such as from students or external parties—this must be clearly indicated. The same applies when AI systems are used in learning management systems.

6. Training & Skills Development

- The university provides ongoing training for safe and trustworthy AI use, including asynchronous online modules.
- Training includes awareness of potential biases, discrimination, and “hallucinations” in AI-generated content.
- It also covers sustainable and digitally sovereign AI use, encouraging preference for European providers and resource-efficient systems.
- Employees are required to familiarize themselves with safe and lawful AI use, relevant regulations, and potential risks before using AI systems in their professional duties.

7. Governance & Responsibility

- The ultimate responsibility for compliant AI use lies with the individual employee or with supervisors/higher authorities who instruct such use.
- The Rectorate appoints an AI Officer within the Prorectorate for IT to oversee policies, training, ethical standards, compliance, audits, and risk assessments related to AI use.
- The AI Systems Whitelist, maintained separately, lists Rectorate-approved AI systems.
- Approval of a new AI system requires involvement of the AI Officer, the Data Protection Office, the Data Protection Officer, and the Information Security Office.

- Before using new AI systems (not yet approved), a review by the AI Officer is mandatory for C2 or higher data.
- Heads of administrative units, central institutions, and scientific departments (e.g. institute or project leaders) are responsible for compliance within their domains and for approving C3 data use in AI systems.

Notes on the EU Artificial Intelligence Act

- Under the EU AI Act, particular attention must be paid to high-risk AI systems, e.g. systems used for automated evaluation of applications, examinations, or admissions. These are subject to strict legal requirements.
- The University of Stuttgart currently does not operate any high-risk AI systems. Should such a system be introduced, prior review by the Rectorate is required, coordinated by the CIO and advised by the AI Officer, Data Protection Office, Data Protection Officer, Information Security Office, and—if necessary—the Ethics Committee.
- For generative AI systems (e.g. chatbots, image generators), the transparency obligations of the EU AI Act are covered by the labeling requirements in this policy.

---

8. Further Development & Feedback

- The Rectorate will review and, if necessary, update this policy at least once per year.
- Suggestions, examples, or questions regarding further development can be sent to ki@uni-stuttgart.de

Validity: Version 1.0, as of October 2025
Responsible unit: AI Officer, Prorectorate for Information Technology