

Prohibited Use Policy

Version 1 - Effective date 1st of May 2026

This Prohibited Use Policy ("Prohibited Use Policy") supplements the General Terms and Conditions of Atelyr B.V. ("Atelyr") and applies to all use of the Software and associated services, including the content that End Customers configure within the Software and the interactions that take place through it. The Prohibited Use Policy applies to both direct and indirect use, within and outside the Software, as well as to any attempts to use the Software in violation of these rules.

Capitalised terms used but not defined in this Prohibited Use Policy have the meaning assigned to them in the General Terms and Conditions.

1. Lawfulness

The Software may only be used for lawful purposes. It is not permitted to use the Software for activities that infringe the intellectual property rights of third parties, violate privacy rights, or involve illegal goods, services, or substances. This includes facilitating the trade in illegal drugs, weapons, hazardous materials, or counterfeit goods, or promoting human trafficking or sexual exploitation.

2. Honesty and Integrity

The Software may not be used for deception, fraud, or abuse. This includes in any event:

Fraud and scams. It is not permitted to use the Software to deceive others, to extract sensitive personal data such as banking details, passwords, or medical information, or to defraud others through financial or other forms of fraud.

Unsolicited communications. It is not permitted to use the Software to contact individuals or businesses at scale and without consent through automated conversations or messages, for "call bombing" or other forms of communication that overload systems or users, or to collect contact details for the purpose of unsolicited communications.

Circumventing security measures. It is not permitted to circumvent security or authentication mechanisms within the Software or at AI Providers.

3. Identity and Transparency

The Software may not be used to impersonate an individual or organisation without their consent, to perform actions on behalf of another party without authorisation, or to harmfully impersonate government

ATELYR

bodies, emergency services, or other authoritative entities. This also includes presenting oneself as an existing company or brand with which the End Customer is not affiliated.

End Customers who deploy AI agents through the Software are required to clearly inform End Users at the start of each conversation or interaction that they are communicating with an automated AI agent and not with a human. This obligation applies regardless of the communication channel.

4. End User Wellbeing

The Software is not intended for applications in which the health, financial situation, or personal integrity of End Users is at stake without adequate supervision. More specifically:

Professional advice. The Software may not be used to provide financial, legal, or medical advice in an automated manner, unless a qualified professional reviews the generated responses before they reach the End User, and unless the End User is clearly informed about the role and limitations of AI in that process.

Gambling and credit. The Software may not be used to facilitate gambling involving real money, or for payday lending services.

Automated decision-making. For applications in which the Software supports decisions that may have a significant impact on an individual's wellbeing, human oversight is required. Fully automated decision-making with such consequences is not permitted.

Manipulative or harmful interactions. The Software may not be used in a manner that exposes End Users to intentionally addictive, manipulative, or otherwise harmful interactions.

5. Child Safety and Sexually Explicit Use

The Software may not be used for sexually explicit conversations, interactions, or applications, regardless of the age of the parties involved.

In particular, the Software may not be used for conversations, interactions, or applications that are sexually explicit and involve minors, or for any other form of exploitation or sexualisation of children, including grooming or using the Software to impersonate a minor. Atelyr will report suspected child abuse to the competent authorities, to the extent required by law or otherwise appropriate.

It is also prohibited to use the Software for interactions that are inappropriate for minors, that promote sexual violence or graphic violence, or that are aimed at intimidating, humiliating, or harming a minor.

6. Hateful, Violent, or Intimidating Use

The Software may not be used for conversations or interactions that threaten, incite, or promote violence, that discriminate on the basis of protected characteristics such as race, religion, gender, or sexual orientation, that intimidate, threaten, or stalk others, or that promote self-harm, suicide, or eating disorders. It is also prohibited to use the Software to spread disinformation, including medical misinformation.

7. Use in Accordance with the Agreement

The Software may only be used within the boundaries of the Agreement. In particular, it is not permitted to:

- resell, sublicense, or otherwise make the Software or its functionalities available to third parties, unless this has been expressly agreed in the context of Atelyr's partner channel;
- use the Software for the development of products or services that compete with Atelyr, or to use the results thereof to the detriment of Atelyr;
- use the Software in a manner that hinders other users or affects the operation, availability, or integrity of the Software;
- decompile, reverse-engineer, or circumvent security measures of the Software;
- create multiple accounts to circumvent usage limits or otherwise obtain financial benefit in violation of the Agreement;
- make the Software available to its own users on terms that are broader than the terms under which Atelyr makes the Software available to the End Customer;
- use the Software in a manner that is contrary to the terms of use or use policies of the AI Provider chosen by the End Customer. End Customers are themselves responsible for familiarising themselves with and complying with the terms of the AI Providers they deploy through the Software;
- use the Software in a manner that qualifies as prohibited or high-risk use within the meaning of the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) or other applicable AI legislation and regulations. End Customers are themselves responsible for assessing their use in light of such regulations.

8. Enforcement

Atelyr assesses potential violations of this Prohibited Use Policy through automated systems, user reports, and human review. In the event of a violation, Atelyr may terminate the relevant use and suspend or terminate access to the Software without entitlement to a refund. The fact that Atelyr does not act in a particular case does not constitute a waiver of rights. In the event of use that poses a risk to individuals, society, or public order, Atelyr reserves the right to inform or cooperate with the competent authorities.

This Prohibited Use Policy does not create rights for third parties and does not give rise to any expectation that use in violation of these rules will be promptly terminated.

Suspected misuse may be reported via support@atelyr.ai. If you believe your account has been incorrectly blocked or suspended, you may contact us at support@atelyr.ai.

9. Amendments

Atelyr may amend this Prohibited Use Policy. Material amendments will be announced in advance. The date of the most recent version is stated at the top of this document.

Atelyr B.V. Dorpsstraat 324A, 1531 HW Wormer, Netherlands

Email: info@atelyr.ai

Website: www.atelyr.ai