NAVICA AI ACCEPTABLE USE POLICY

Effective: 10 August 2026

This standalone policy forms part of the Navica AI Platform Contract.

Information about Navica

This policy is provided by Navica Italy S.r.l., registered number 03074050992, of Salita dei Sassi 7/2, 16128 Genova, Italy, and its affiliates. Contact abuse@navica.ai about this policy.

Definitions

- “Applicable Law” means all laws and binding regulatory requirements applicable to the relevant use of the Platform or Services.
- “AI Output” means content, analysis, recommendations, configurations, models, workflows, code or other output generated through the Platform’s artificial-intelligence capabilities.
- “High-Risk Use” means a use of an AI system classified as high-risk under applicable AI laws.
- “Platform” means the Navica platform available at navica.ai and through related applications.
- “Services” means the services Navica makes available through or in connection with the Platform.
- Other capitalised terms have the meanings given in the Navica AI Platform Terms of Service.

Policy

This Acceptable Use Policy ("AUP") applies to anyone who accesses or uses the Platform or Services. By accessing and using the Platform and/or Services, you agree to be bound by this AUP and to comply with its terms. If you do not agree to be bound by this AUP, you must not access or use the Platform or Services.

This AUP is provided by Navica Italy S.r.l. (a company incorporated in Italy with registered number 03074050992 and registered office at Salita dei Sassi 7/2, 16128 Genova, Italy) and its affiliates (together referred to as “Navica”, “we”, “us” or “our”). Contact Navica about this AUP at abuse@navica.ai.

A1. Prohibited Uses

You shall not use the Platform or Services:

To violate any Applicable Law or in a manner that breaches Navica’s policies, frameworks or documentation

To generate, distribute, or facilitate the creation of content that is unlawful, defamatory, fraudulent, obscene, or harmful

In any manner that would infringe or misappropriate any third party's intellectual property, privacy, or proprietary rights

In any way that would impersonate any person or entity or misrepresent your affiliation

To transmit malware, viruses, or any code designed to disrupt or damage the Platform or Services or use the Platform or Services in such a way these could be knowingly or recklessly introduced

To attempt to gain unauthorised access to the Platform, other users' accounts, or connected systems

To make automated decisions in regulated contexts (employment, credit, insurance, healthcare, maritime safety) without Navica’s prior written authorisation (and any use is strictly subject to the conditions imposed by Navica which may include appropriate human oversight)

In any safety-critical application without Navica’s prior written authorisation (and any use is strictly subject to the conditions imposed by Navica which may include implementing appropriate safeguards, validation procedures, and human oversight)

To reverse engineer, extract, reconstruct, or attempt to determine model weights, training data, algorithms, source code or system logic underlying the Platform (its models) or the Services

In a way that circumvents any usage limits, access controls, or security measures or which disables or bypasses these

In any manner that could disable, overburden, or impair the Platform or Services or disrupt its integrity or performance

To develop a competing product or service or provide services to third parties

In any manner that would damage the reputation or Navica or bring it into disrepute or conflict

A1.1 Unlawful AI and Abuse

You shall not use, configure, distribute or enable the Platform, AI Output or any integrated AI system for:

Any Prohibited AI Practice or other use prohibited by Applicable Law

Fraud, harmful manipulation, deception, impersonation or exploitation

Unlawful surveillance, biometric processing, profiling, doxxing, stalking or other privacy violations

Malware, phishing, credential theft, unauthorised exploitation or other cyber abuse

safety-critical use unless Navica has provided its prior written authorisation (and any such use is strictly subject to Navica's conditions which may include conditions in relation to appropriate validation, professional review, safeguards and human oversight)

In relation to your use of AI Output, the following conditions apply:

You are solely responsible for determining whether AI Output is suitable for its intended use and any reliance on the AI Output is at your discretion. You further agree not to use AI Output as the sole basis for operational decisions without independent professional verification including where such decisions may affect health, safety, or the environment.

You acknowledge that AI Output is probabilistic and may be similar or identical to output generated for other users who submit similar inputs

You acknowledge and agree that Navica makes no representation that AI Output qualifies for copyright or other intellectual-property protection under Applicable Law

You acknowledge that AI Output may contain hallucinations, errors, incomplete statements, bias, untruthful content or unsupported information or be misleading

A1.2 High-Risk Uses Require Written Approval

You shall not use the Platform for a High-Risk Use unless the use case has been disclosed to Navica and you have obtained Navica's prior authorisation (and this must be recorded in writing whether in an Order Form, High-Risk Use Addendum or other written document). Navica may require additional documentation, safety controls, audit logs, human oversight, technical testing, regulatory evidence, insurance or professional qualification evidence as a condition of approval.

A2. Safety Tools and Governance Obligations

A2.1 Prohibited Safety Practices

You shall not:

Disable, bypass, tamper with, or remove Safety Tools, guardrails, verification frameworks, or audit controls for the purpose of avoiding safety checks or accelerating processes at the expense of safety

Deploy agents, workflows, or operational models in safety-critical production environments without first obtaining Navica's prior written authorisation (and any such deployment or use is subject to Navica's conditions which may require, without limitation, conducting appropriate verification and validation testing)

Conceal, alter or delete audit-log entries

Configure agents or workflows to circumvent human-in-the-loop controls where such controls are required by Applicable Law, regulation, or industry standard or by Navica

Misrepresent the level of human oversight or safety governance applied to AI-assisted processes to regulators, customers, or other third parties

A3. Compliance with Industry Regulations

Customers in regulated industries are responsible for compliance with applicable industry-specific regulations, standards and professional requirements. Safety Tools, audit logs and governance frameworks may assist but do not guarantee compliance.

A4. Reporting and Enforcement

Report suspected AUP violations, safety incidents, security vulnerabilities, governance concerns or other issues with the Platform and Services (including that AI Output contains errors) to abuse@navica.ai. Navica may investigate and take appropriate action, including suspension or termination, mandatory remediation and referral to law enforcement or regulators.

A5. Breaches

In the event that you do not comply with the terms of this AUP, Navica reserves the right to take action against you which includes suspending or withdrawing your access to and use of the Platform and Services (or any part thereof).