

Acceptable Use Policy for Parloa

This Acceptable Use Policy ("Policy") applies to all users of the Parloa Platform and governs the use of the services provided by Parloa ("Services"). By accessing the Parloa Platform and using Parloas Services, you as a "User" agree to the terms set forth in this Policy.

Now therefore, the Parties agree as follows:

1. User Responsibilities for Using Parloa Services

- 1.1. You are granted access to the Services based on an "Agreement" between the Parloa entity (as shown on the respective Agreement) and the partner or customer responsible for providing you with access rights. Your use of the Services is subject to the terms and conditions set forth in that Agreement.
- 1.2. As a User of Parloa's Services, you must ensure the following:
 - 1.2.1. Password Security: Use a secure and confidential password to access the Services.
 - 1.2.2. Compliance and Lawful Use: Use the Services in accordance with the terms and conditions of the Agreement, signed with the Parloa Entity . Ensure compliance with all applicable laws and regulations in your activities under the Agreement. Only use the Services for lawful purposes.
 - 1.2.3. Prevention of Unauthorized Access: Make commercially reasonable efforts to prevent any unauthorized access to, or use of, the Services. Promptly notify Parloa in the event of any unauthorized access or use.
 - 1.2.4. Accuracy and Responsibility of Data: You are solely responsible for the accuracy, completeness, design, appropriateness, creation, maintenance, and updating of all data you use with the Services.
 - 1.2.5. Parloa is not liable for any errors or inaccuracies in:
 - Any information you provide.
 - Any of your data.
 - Any changes or modifications to your data made by Parloa upon your written instructions, beyond Parloa's responsibility to accurately reproduce such data upon your instruction.
- 1.3. Supported Browser: Use a supported browser to access the Platform.
- 1.4. Licenses and Consents: Obtain all necessary licenses and consents required to use your data within the agreed scope, including those from third-party information owners or licensees. Warrant and represent that such licenses and consents have been obtained.
- 1.5. Platform Usage Limitation: Acknowledge that the Platform serves to distribute and syndicate your data but does not serve as a storage solution for your data and should not be used in this way.
- 1.6. Prohibited Activities:

Do not upload, input, access, store, distribute, or transmit any viruses or any material that:

 - Is unlawful, infringes on intellectual property rights, privacy rights, or any other rights

of others.

- Does not comply with data protection or privacy regulations (GDPR) or any other applicable law for the data you provide.
 - Abuses Platform features or includes harmful, threatening, defamatory, obscene, infringing, harassing, or racially or ethnically offensive content.
 - Facilitates illegal activities, including distributing files infringing copyrights or holding malicious software.
 - Depicts sexually explicit images or includes offensive, defamatory, discriminatory, or otherwise inappropriate content.
 - Promotes unlawful violence or discrimination based on race, gender, color, religious belief, sexual orientation, disability, or any other illegal activity.
 - Causes damage or injury to any person or property.
 - Creates fake identities or accounts, impersonates other individuals or entities in misleading or deceptive manners.
 - Involves unauthorized data mining or collection of users' private information or sending unsolicited bulk communications.
- 1.7. Jurisdiction and Sanctions Compliance: Do not access or use the Services if you are located in a jurisdiction subject to U.S. or EU economic sanctions.
- 1.8. Do not provide access to the Services to any government, entity, or individual located in any such jurisdiction or to any individual identified on any U.S. or EU sanctions lists.
- 1.9. Provider Rights: Parloa reserves the right, without liability or prejudice to its other rights, to:
- Disable your access to any material that breaches the provisions of this section.
 - Disable the Services in respect of any content that, in Parloa's sole and reasonable discretion, is suspected to be in violation of this section.
 - Disable your account with regard to any content in violation of this section and inform you accordingly.
- 1.10. User Privacy: Our service uses the following tools for tracking and improving our product and engineering efforts. All tracking is conducted in an anonymized manner where possible:
- PostHog - For anonymized tracking to improve our product.
- Datadog - For anonymized tracking to support engineering and operational purposes.
- Google Fonts - Used for font rendering across the platform.
- Google Tag Manager - to analyze and improve the platform's usage
- Auth0 - For user authentication and authorization

2. User Responsibilities for Using AI Services

Parloa provides Services with the use of artificial intelligence and machine learning services, features, and functionality (including third-party models) (collectively "AI Services").

- 2.1. As a User, you may not use, or facilitate or allow others to use, AI Services:

- Interacting with individuals below the legal age of consent in ways that could lead to exploitation, manipulation, or any actions prohibited by law or regulation.
- Generating or using content that is prohibited by this Acceptable Use Policy, as well as monetizing such content or presenting it alongside other content.
- Making decisions without proper human oversight that could impact an individual's legal or financial status, life opportunities, employment opportunities, or human rights, or that could result in physical or psychological harm.
- Employing subliminal techniques intended to deceive or cause harm.
- Intentionally misleading, manipulating, or spreading false information, including false advertising and exploiting vulnerabilities such as age or socio-economic status.
- Conducting social scoring, predictive profiling, or categorizing individuals based on sensitive attributes such as race, political opinions, or sexual orientation.
- Creating, sharing, or engaging with content that attacks, denigrates, intimidates, degrades, targets, or excludes individuals or groups based on traits such as actual or perceived race, ethnicity, national origin, gender, gender identity, sexual orientation, religious affiliation, age, disability status, caste, or any other characteristic associated with systemic prejudice or marginalization.
- Inferring emotions or sensitive attributes from physical, physiological, or behavioral characteristics, such as facial expressions or speech patterns.
- Creating or operating chatbots for erotic, romantic, or other purposes prohibited by this Acceptable Use Policy, including impersonating specific individuals without their explicit consent or claiming to possess special wisdom without clearly labeling it as entertainment.
- Identifying or verifying individuals based on biometric data without approval for modified content filtering or using such data for unlawful surveillance, tracking, or harassment.
- Using facial recognition technology for police or law enforcement purposes, especially in uncontrolled environments or for real-time identification, without the necessary legal consent.
- Generating content with the intent to remove or alter AI Content Credentials to mislead others or detecting AI Content Credentials without authorization.
- Engaging in the dissemination of intentional disinformation, violating privacy rights, unauthorized depiction of a person's likeness, or any form of harm or abuse, especially toward minors.
- Intentionally circumventing safety filters or prompting models to act in a manner that violates these policies.
- Using content that supports unlawful active attacks or malware campaigns that cause technical harms, such as delivering malicious executables, organizing denial of service attacks, or managing command and control servers.
- For intentional disinformation or deception.
- To violate the privacy rights of others, including unlawful tracking, monitoring, and identification.

- To depict a person's voice or likeness without their consent or other appropriate rights, including unauthorized impersonation and non-consensual sexual imagery.
- For harm or abuse of a minor, including grooming and child sexual exploitation.
- To harass, harm, or encourage the harm of individuals or specific groups.
- Use content that depicts, endorses, supports, promotes, glorifies, encourages, or instructs individuals to engage in acts of violence, harm others, or commit illegal activities.

These content requirements apply universally to the use of AMP by Parloa and all included Microsoft Generative AI Services to ensure the protection and safety of individuals and society.

Users are permitted to provide, generate, classify, collect, and filter content that would otherwise violate this Acceptable Use Policy solely (1) to evaluate, train, and improve safety systems and applications for their own use, as permitted by any agreement between Parloa and the User, and (2) to evaluate and test AMP in accordance with the Agreement. Any harmful content generated during this process may be used solely for evaluation and reporting purposes and not for any other purpose. Users remain responsible for all legal compliance related to such content, including retention, destruction, and reporting as required.

- 2.2. If you use the AI Services to make consequential decisions, you must evaluate the potential risks of your use case and implement appropriate human oversight, testing, and other use case-specific safeguards to mitigate such risks. Consequential decisions include those impacting a person's fundamental rights, health, or safety (e.g., medical diagnosis, judicial proceedings, access to critical benefits like housing or government benefits, opportunities like education, decisions to hire or terminate employees, or access to lending/credit, and providing legal, financial, or medical advice). You agree to provide information about your intended uses of the AI Services and compliance with this Policy upon request.
- 2.3. You and your end users are responsible for all decisions made, advice given, actions taken, and failures to take action based on your use of AI Services. AI Services use machine learning models that generate predictions based on patterns in data. Output generated by a machine learning model is probabilistic, and generative AI may produce inaccurate or inappropriate content. Outputs should be evaluated for accuracy and appropriateness for your use case.
- 2.4. Parloa may investigate and enforce violations of this Policy. Parloa is committed to developing safe, fair, and accurate AI Services and providing you with tools and guidance to assist you in building and using AI Services responsibly. See our [Responsible AI Policy](#) (available on our [Trust Centre](#)) for further details.

3. Parloa Intellectual Property Rights and Licenses

Except as may be permitted by applicable law, User shall not:

- make alterations to, or modifications of, the whole or any part of the Services or permit the Services or any part of it to be combined with, or become incorporated in, any other programs;
- disassemble, decompile, reverse-engineer or create derivative works based on the whole or any part of the Services or attempt to do any such thing;
- copy, frame, or mirror any part of the Services;
- access all or any part of the Services or the Documentation in order to build a Platform or service which competes with the Services or the Documentation;
- provide, commercially exploit or otherwise make available the Services, in any form to any

person;

- use the Services or the Documentation to provide the Services or certain functionalities thereof to third parties, except where expressly agreed otherwise in writing by the duly authorized representatives of Provider.

4. Parloa's Rights

- 4.1. Parloa may, at times, restrict AMP's ability to respond to certain topics, including requests for personal information or inquiries about sensitive subjects or current events, even if such topics are not explicitly prohibited by this Acceptable Use Policy.
- 4.2. Violations of this Acceptable Use Policy may result in a range of consequences, including but not limited to: suspension or termination of access to AMP by Parloa, revocation of licenses or subscriptions, removal of prohibited content, legal action, and reporting of the violation to appropriate authorities. Parloa reserves the right to take any necessary actions to protect its services, users, and the broader community, and to ensure compliance with this policy.

5. Reporting

If you suspect that AMP by Parloa is being used in an abusive or illegal manner, infringes on your rights or the rights of others, or violates this Acceptable Use Policy, you can report it through Support Portal.

6. Legal Basis

This policy will be reviewed by the Responsible AI Committee annually or as needed, based on the evolution of AI technology and the regulatory landscape. Any changes to the policy will be communicated to all Users.