Amplience Acceptable Use Policy (AUP)

ACCEPTABLE USE POLICY

Effective Date: [Date]

Last Updated: [Date]

This Acceptable Use Policy ("Policy") sets forth the rules and guidelines governing access to and use of the Amplience SaaS Solution ("Service"). By accessing or using the Service, you ("Customer") agree to comply with this Policy. Any violation of this Policy may result in suspension or termination of access to the Service, in addition to any other remedies available under the Agreement.

Rate Limiting

Customer shall not:

- Use the Service in a manner that results in sustained high-volume API traffic or automated usage that negatively impacts the performance or stability of the Service.
- Exceed rate limits as defined at https://amplience.com/developers/docs/apis/limits (the "Default Rate Limits"), which shall serve as the default rate limits, unless alternative limits are specified in the Order Form or otherwise mutually agreed in writing.
- Employ bots, crawlers, scripts, or automated systems that simulate user interaction to circumvent rate-limiting mechanisms.
- Conduct or facilitate high-volume or coordinated traffic patterns (malicious or otherwise) from a particular network or region without authorisation.

Domain and Channel Restrictions

Customer may only use the Service to deliver content to domains and channels expressly authorised in an accepted Order Form. Specifically, Customer shall not:

- Serve or distribute content generated by the Service to any domain or channel not approved in writing by Amplience.
- Distribute or proxy content from the Service to third-party sites or services without prior written authorisation.
- Use the Service on domains not owned or controlled by Customer or for purposes of resale, unless contractually permitted.

4. Prohibited Content and Data Use

Customer shall not upload, publish, store, or transmit through the Service any content or data that:

- Is not owned by Customer or for which Customer does not have sufficient legal rights or licenses.
- Includes personal data that is not intended for public viewing, unless express, informed consent has been obtained from the data subject.
- Includes special category personal data as defined in Article 9 of Regulation (EU) 2016/679 (GDPR), including but not limited to health data, biometric data, or political opinions.
- Contains or is intended to propagate malicious code, viruses, or any other harmful software or logic.

5. Security and Access Control

Customer shall not:

- Conduct or commission any security testing (including but not limited to penetration testing or load testing) of the Service without prior written consent from Amplience.
- Use temporary or disposable email addresses for user accounts or share user credentials among multiple individuals.
- Disclose access credentials or authentication tokens to any third party.
- Impersonate any individual or entity in connection with use of the Service.

6. Usage Scope and Licensing Restrictions

Customer shall not:

- Share, sell, license, rent, lease, or otherwise provide access to the Service or any portion thereof, including components, deliverables, or Provider products, to any third party.
- Develop, create, or distribute derivative works based on the Service, its deliverables, or any associated proprietary or confidential information.
- Modify, tamper with, bypass, or interfere with any part of the Service or its technical infrastructure.
- Grant any third party any security interest, lien, or encumbrance in or over the Service or any portion thereof.
- Share, upload, or store confidential Amplience information or data in third-party procurement, marketplace, or comparison platforms without express written authorisation.

7. Reverse Engineering and Intellectual Property

Customer shall not:

- Decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code, object code, or underlying structure of the Service or any Amplience product or deliverable, except to the limited extent expressly permitted by applicable law and not waivable by contract.

8. AWS Acceptable Use Policy

Customer must abide by the terms outlined in the AWS Acceptable Use Policy (available at https://aws.amazon.com/aup/).

9. Responsibilities

Customer agrees to:

- Promptly report any actual or suspected security vulnerabilities, data leaks, service misuse, or unauthorised access related to the Service by emailing security@amplience.com or another method explicitly identified by Amplience.
- Not publicly disclose any vulnerability affecting the Service without first providing Amplience with reasonable advance notice and sufficient detail to investigate and mitigate the issue.
- Cooperate in good faith with any investigation conducted by Amplience concerning service misuse, security incidents, or potential violations of this Policy.
- Keep all access credentials secure and confidential, and notify Amplience immediately of any known or suspected unauthorised use of the Service or compromise of access credentials.

- Ensure that its end users, agents, or contractors using the Service are aware of and adhere to this Policy.

10. Enforcement

Amplience reserves the right to limit, restrict, or block access to the Service where a breach of this Policy is identified. Wherever practicable, Amplience will make reasonable efforts to notify the Customer in advance of enforcement actions. However, if continued activity presents a risk to the stability, performance, or security of the Service, Amplience may take immediate action without prior notice, and without liability or financial recourse to the Customer.

Such enforcement measures may include, but are not limited to:

- Applying rate limiting to individual IP addresses, CIDR ranges, or behavioural signatures.
- Triggering CAPTCHA or similar human verification mechanisms.
- Blocking traffic originating from specific ASNs (Autonomous System Numbers).
- Disabling one or more API keys associated with the Customer.
- Applying automated or manual configuration adjustments to reduce the quality, resolution, or payload size of media content including images and videos.

These measures will be employed in a manner proportionate to the threat or policy violation and may be temporary or permanent depending on the circumstances.

11. Reporting Violations

If you become aware of any activity that violates this Acceptable Use Policy, including misuse of the Service, unauthorised access, or suspected security vulnerabilities, you are encouraged to report it promptly.

Violations can be reported by contacting:

- Email: security@amplience.com
- Support Channels: via your account representative or Amplience Support Portal (available at https://support.amplience.com)

Reports should include as much relevant detail as possible, including:

- A description of the violation or suspicious activity
- Date and time of the observed behaviour
- Relevant IP addresses, API keys, or domain names
- Any logs, headers, or payloads (as applicable and permissible)

All reports will be treated confidentially. Amplience may follow up for additional information as necessary and reserves the right to take appropriate action in accordance with this Policy and the governing Agreement.

12. Amendments and Enforcement

Amplience reserves the right to modify this Policy at any time. Continued use of the Service following such modifications constitutes acceptance of the revised terms. Amplience may monitor compliance and may suspend or terminate access to the Service in response to any violation of this Policy.

Amplience Acceptable Use Policy (AUP)