Acceptable Use Policy

Last Updated: *May 13, 2024*
Effective Date: *May 20, 2024*

Our customers rely on Braze to keep the Braze Services running without disruption and to provide guidance on legal requirements and industry best practices. This Acceptable Use Policy (**"AUP**") sets forth how the Braze Services must be used, and more importantly, what constitutes misuse of the Braze Services, either because the activity violates applicable law, or because it poses a risk to the Braze Services. Terms used herein without definition are defined in the subscription agreement ("**Agreement**") in place between Braze (or a Braze Reseller) and its customers.

Updates to the AUP: Braze reserves the right to update this AUP in accordance with industry best practices and applicable law by posting a revised copy on this webpage. Customers can subscribe to receive notification of updates by clicking the "**Subscribe for AUP Updates**" button below.

AUP violations: A violation of this AUP shall be deemed a breach of the Agreement and may result in Braze's refusal to send Messages or in the suspension and/or termination of Customer's subscription to use the applicable services. Braze will provide a written basis for any suspension or termination.

1. MESSAGING POLICY

Messaging includes the sending of Email Messages, SMS/MMS Messages, and any other electronic Messages sent through the Braze Services. All Messages sent via the Braze Services must comply with applicable laws, applicable Third-Party Provider terms of use, and industry standards.

- Customer shall not: (i) send Messages that result in excessive spam or complaints, bounces, spam trap hits, unsubscribes, blocklistings, or other poor deliverability outcomes (even if the Messages themselves are not actually spam), or (ii) employ sending practices that negatively impact Braze or its customers.

- Customers shall not send unsolicited Messages. You must have evidence of consent for any commercial or marketing Messages sent through the Braze Services. Customer may not send Messages to (i) purchased, appended or rented lists, (ii) email addresses or phone numbers programmatically generated or scraped from the internet, (iii) role-based or non-specific addresses (e.g., webmaster@domain.com or info@domain.com), (iv) list-servers or distribution addresses, or (v) lists generated through co-registration programs.

- All Email Messages must include a visible and working unsubscribe mechanism that complies with industry best practices.

- Messages may not:
    - Disguise the origin or subject matter of the message, or contain a falsified or manipulated "from" address, subject line, header, or transmission path information; and
    - Contain links to phishing sites or content related to pyramid schemes, multi-level marketing opportunities, affiliate marketing, or any other content that is reasonably likely to be tortious, libelous, deceptive, fraudulent, infringing, harassing, harmful, obscene, or abusive ("**Malicious Content**"). For purposes of this section, affiliate marketing shall refer to a business model in which marketers are paid commissions to generate leads or sales for a third party, or similar arrangements, and their partners do not have explicit permission to mail recipients.

- Customer must have a publicly-available privacy policy for all active sending domains that complies with applicable laws and Third-Party Provider terms of use.

- Customer's messaging policy must explicitly state that opt-in data will not be shared with third parties.

SMS/MMS Messages

In addition to the above, when sending SMS/MMS Messages:

- Customer must comply with the SMS/MMS Providers' applicable acceptable use and prohibited content messaging policies (including without limitation, those of Twilio and Infobip), applicable industry standards and guidelines, including the CTIA Messaging Principles and Best Practices and applicable carrier (*e.g.,* AT&T, T-Mobile, etc.) guidelines and/or codes of conduct; and
- Customers in the US and applicable countries are prohibited from sending SMS/MMS Messages that contain content related to Sex, Hate, Alcohol, Firearms, Tobacco/CBD (S.H.A.F.T. regulations or guidelines).

2. REASONABLE USAGE

If Customer exceeds its entitlements or attempts to process more data through the Braze Services than reasonably expected based on Customer's entitlements and package (e.g., abusive data processing or unduly burdensome data processing through the Braze Services), Braze may manage data processing traffic in order to preserve the overall stability of the Braze Services.

3. PROHIBITED ACTIVITIES

Customers shall not take actions that may threaten the security, stability, or availability of the Braze Services, including:

- Overwhelming the Braze infrastructure by imposing an unreasonably large load on the Braze Services (i.e., using "robots," "spiders," "offline readers," or other automated systems to send more request messages to the Braze Services than a human could reasonably send in the same period of time by using a normal browser);
- Going beyond the use parameters for any given product or feature, as described in the Documentation;
- Consuming an unreasonable amount of storage for music, videos, or any other materials in a way that is unrelated to the purposes for which the Braze Services were designed;
- Attempting to probe, scan or test the vulnerability of the Braze Services; and
- Accessing any part of the Braze Services by any means other than our publicly-supported interfaces (for example, "scraping").

4. EXTERNAL-FACING SERVICES

Customer shall not display on any external-facing Braze Services any Malicious Content and/or content that violates the intellectual property rights or other rights of third parties (such as confidentiality, publicity or privacy rights) or applicable laws.

Customer shall identify itself clearly as the recipient of any data or information collected by Customer through any external-facing Braze Services.