Messaging SaaS Policy

This oneapp Messaging SaaS Policy applies to SMS, MMS, Chat, and WhatsApp messaging channels. We all expect that the messages we want to receive will reach us, unhindered by filtering or other blockers. An important step oneapp and our customers can take to make that expectation reality is to prevent and eliminate unwanted messages. Towards that end, we strive to work with our customers so that messages are sent with the consent of the message recipient, and that those messages comply with applicable laws, communications industry guidelines or standards, and measures of fairness and decency.

This principle is central to oneapp's Acceptable Use Policy.

oneapp Messaging SaaS

oneapp treats all messaging transmitted via oneapp's platform - regardless of use case or phone number type (e.g., long code, short code, or toll-free) - as Application-to-Person (A2P) messaging. All A2P messages originating from oneapp's platform are subject to this oneapp Messaging SaaS Policy, which covers rules and /or prohibitions regarding:

- Consent ("opt-in");
- Revocation of Consent ("opt-out");
- Sender Identification;
- Messaging Usage;
- Filtering Evasion; and
- Enforcement.

This policy applies to all customers who use oneapp's messaging channels. If you provide your own end users or clients with the ability to send messages through oneapp, for example as an ISV ("Independent Software Vendor"), you are responsible for the messaging activity of these users. You must ensure that any messaging activity generated by your users is in compliance with oneapp policies.

Consent/Opt-in

What Is Proper Consent?

Consent can't be bought, sold, or exchanged. For example, you can't obtain the consent of message recipients by purchasing a phone list from another party.

Aside from two exceptions noted later in this section, you need to meet each of the consent requirements listed below. If you are a software or platform provider using oneapp's platform for messaging within your application or service, you must require your customers to adhere to these same requirements when dealing with their users and customers.

Consent Requirements

- Prior to sending the first message, you must obtain agreement from the message recipient to communicate with them - this is referred to as "consent", you must make clear to the individual they are agreeing to receive messages of the type you're going to send. You need to keep a record of the consent, such as a copy of the document or form that the message recipient signed, or a timestamp of when the customer completed a sign-up flow.

- If you do not send an initial message to that individual within a reasonable period after receiving consent (or as set forth by local regulations or best practices), then you will need to reconfirm consent in the first message you send to that recipient.
- The consent applies only to you, and to the specific use or campaign that the recipient has consented to. You can't treat it as blanket consent allowing you to send messages from other brands or companies you may have, or additional messages about other uses or campaigns.
- Proof of opt-in consent should be retained as set forth by local regulation or best practices after the end user opts out of receiving messages.

Alternative Consent Requirements

While consent is always required and the consent requirements noted above are generally the safest path, there are two scenarios where consent can be received differently.

Contact initiated by an individual

If an individual sends a message to you, you are free to respond in an exchange with that individual. For example, if an individual texts your phone number asking for your hours of operation, you can respond directly to that individual, relaying your open hours. In such a case, the individual’s inbound message to you constitutes both consent and proof of consent. Remember that the consent is limited only to that particular conversation. Unless you obtain additional consent, don't send messages that are outside that conversation.

Informational content to an individual based on a prior relationship

You may send a message to an individual where you have a prior relationship, provided that individual provided their phone number to you, and has taken some action to trigger the potential communication, and has not expressed a preference to not receive messages from you. Actions can include a button press, alert setup, appointments, or order placements. Examples of acceptable messages in these scenarios include appointment reminders, receipts, one-time passwords, order/shipping/reservation confirmations, drivers coordinating pick up locations with riders, and repair persons confirming service call times.

The message can't attempt to promote a product, convince someone to buy something, or advocate for a social cause.

Periodic Messages and Ongoing Consent

If you intend to send messages to a recipient on an ongoing basis, you should confirm the recipient’s consent by offering them a clear reminder of how to unsubscribe from those messages using standard opt-out language (defined below). You must also respect the message recipient’s preferences in terms of frequency of contact. You also need to proactively ask individuals to reconfirm their consent as set forth by local regulations and best practices.

Identifying Yourself as the Sender

Every message you send must clearly identify you (the party that obtained the opt-in from the recipient) as the sender, except in follow-up messages of an ongoing conversation.

Opt-out

The initial message that you send to an individual needs to include the following language: “Reply STOP to unsubscribe,” or the equivalent using another standard opt-out keyword, such as STOPALL, UNSUBSCRIBE, CANCEL, END, and QUIT.

Individuals must have the ability to revoke consent at any time by replying with a standard opt-out keyword. When an individual opts out, you may deliver one final message to confirm that the opt-out has been processed, but any subsequent messages are not allowed. An individual must once again provide consent before you can send any additional messages.

Usage Limitations

Content We Do Not Allow

The key to ensuring that messaging remains a great channel for communication and innovation is preventing abusive use of messaging platforms. That means we never allow some types of content on our platform, even if our customers get consent from recipients for that content. The oneapp Acceptable Use Policy prohibits sending any content that is illegal, harmful, unwanted, inappropriate, objectionable, confirmed to be criminal misinformation, or otherwise poses a threat to the public, even if the content is permissible by law. Other prohibited uses include:

- Anything that is illegal or otherwise unlawful in the jurisdiction where the message recipient lives.
- Hate speech, harassment, exploitative, abusive, or any communications that originate from a hate group.
- Fraudulent messages.
- Malicious content, such as malware or viruses.
- Any content that is designed to intentionally evade filters (see below).

Area-Specific Rules

All messages should comply with the rules applicable to the area in which the message recipient lives, which may be found in our SaaS and Area Specific Requirements.

Age and Geographic Gating

If you are sending messages in any way related to adult content, then more restrictions apply. In addition to obtaining consent from every message recipient, you must ensure that no message recipient is younger than the legal age of consent based on where the recipient is located. You also must ensure that the message content complies with all applicable laws of the jurisdiction in which the message recipient is located or applicable communications industry guidelines or standards.

You need to be able to provide proof that you have in place measures to ensure compliance with these restrictions.

oneapp Messaging SaaS Policy Violation Detection and Prevention Evasion

Customers may not use oneapp’s platform to evade oneapp’s or a telecommunications provider’s unwanted messaging detection and prevention mechanisms. Subject to oneapp’s Privacy Notice, oneapp collects and monitors the content of text messages that are transmitted via oneapp’s platform to certain areas in order to detect spam, fraudulent activity, and violations of the oneapp Acceptable Use Policy.

Examples of prohibited practices include:

- Content designed to evade detection. As noted above, we do not allow content which has been specifically designed to evade detection by unwanted messaging detection and prevention mechanisms. This includes intentionally misspelled words or non-standard opt-out phrases which have been specifically created with the intent to evade these mechanisms.
- Snowshoeing. We do not permit snowshoeing, which is defined as spreading similar or identical messages across many phone numbers with the intent or effect of evading unwanted messaging detection and prevention mechanisms.

- Simulated social engineering attacks. You are prohibited from transmitting messages that are used for security testing, including simulated phishing and other activities that may resemble social engineering or similar attacks.
- Other practices identified and prohibited by this policy and oneapp's Acceptable Use Policy.

How We Handle Violations

When we identify a violation of these principles, where possible, we will work with customers in good faith to get them back into compliance with this policy. However, to protect the continued ability of all our customers to freely use messaging for legitimate purposes, we reserve the right to suspend or remove access to oneapp's platform for customers or customers' end users' that we determine are not complying with the oneapp Messaging SaaS Policy, or who are not following the law in any applicable area or applicable communications industry guidelines or standards, in some instances with limited notice in the case of serious violations of this policy.