Email SaaS Policy

This oneapp Email SaaS Policy (“Email SaaS Policy”) applies to oneapp Email SaaS (“oneapp Email Saas”). This Email SaaS Policy provides the restrictions and requirements you must abide by to use the oneapp Email SaaS. This Email SaaS Policy applies to you and your organization, end users, and customers, and any references to “you” in this Email SaaS Policy includes your organization, end users, and customers. These restrictions and requirements ensure that all emails sent via the oneapp Email SaaS are safe, wanted, and legal.

This Email SaaS Policy applies in addition to, and forms part of, oneapp's Acceptable Use Policy, which you are encouraged to read.

Affirmative Consent (“opt-in”) Requirements

Except for transactional emails (i.e., non-marketing emails that contain information about an action or transaction a recipient has taken or agreed to and, if applicable, updates or notifications to that recipient about that action or transaction), you must obtain affirmative consent prior to sending any emails to a recipient via the oneapp Email SaaS. Any affirmative consent must be freely given by each recipient to each sender (e.g., blanket consents or consents provided on behalf of a third party are not acceptable), informed, and unambiguous. This means a recipient must be (a) presented with the choice to provide or withhold consent; (b) informed of the sender’s identity (see Sender Identification paragraph below), how its email address will be used, and the subject matter of the emails it will receive; and (c) made aware of how to withdraw, at any time, any previously provided affirmative consent. You must obtain affirmative consent from a recipient again if you send that recipient an email after an extended period of non-engagement.

Any affirmative consent that you obtain from a recipient is strictly for the subject matter for which that recipient provided that affirmative consent. Please also note that any affirmative consent that you obtain is not transferable to your affiliates or any other party.

You are required to retain proof of all affirmative consents obtained from recipients at least until the recipient withdraws its affirmative consent. Upon written request from oneapp, you must promptly provide proof of a recipient’s affirmative consent and the date and the method through which that recipient’s email address was obtained.

Sender Identification Requirements

Each email that you send via the oneapp Services must (a) clearly identify and accurately represent the sender (i.e., the party that obtained the affirmative consent from a recipient or the party that is initiating the transmission of the email) and (b) include a clear non-deceptive subject line, which accurately describes the content and purpose of the email (e.g., if the email is an advertisement or a promotion, the subject line should clearly reflect this).

Revocation of Affirmative Consent (“opt-out”) Requirements

Except for transactional emails (as defined above), the body of each email that you send via the oneapp Services must include (a) an active and accurate physical mailing address where a recipient can send an unsubscribe request via mail; (b) clear, conspicuous, and functioning unsubscribe hyperlink; and (c) a hyperlink to your privacy policy applicable to the emails you send.

A recipient must have the ability to revoke its affirmative consent at any time. You must honor all affirmative consent withdrawal requests within (10) days of the date they are sent, or the timeframe required under applicable law or regulation, whichever is shorter. You may not send emails to a recipient that has withdrawn its affirmative consent, unless that recipient provides its subsequent affirmative consent. This paragraph does not apply to transactional emails (as defined above).

Prohibited Content

The following content is prohibited from being sent via the oneapp Email SaaS:

- Pornography or sexually explicit content;
- Escort services, mail-order bride or spouse finders, international marriage brokers, and other similar services;
- Statements about products claiming to prevent, treat, or cure health issues (e.g., illness or disease) that have not been approved by the applicable government authority or are not permitted under applicable law or regulation;
- Advertising for prescription medication that cannot legally be sold over-the-counter; and
- Content that is fraudulent or that oneapp determines in good faith is intended to mislead a recipient (e.g., phishing emails, chain letters, pyramid schemes) or cause harm or damage (e.g., malware or viruses).

Prohibited Actions

You are prohibited from using the oneapp Email SaaS in the following ways:

- Sending unsolicited or unwanted emails in bulk;
- Sending emails to email addresses that you obtained from the Internet or social media or to generic email aliases (e.g., webmaster@domain.com or info@domain.com) without obtaining prior affirmative consent;
- Using third-party email addresses and domain names without proper consent or authorization from the third party;
- Using or embedding tracking technologies (e.g., tracking pixels or cookies) in emails sent to a recipient prior to obtaining consent from that recipient to the extent and in the manner required by applicable law or regulation;
- Using purchased or rented email lists or email lists of recipients that have not affirmatively consented to receive emails from you;
- Using techniques or practices to evade mechanisms, filters (e.g., spam filters), and detection capabilities (e.g., anti-abuse or spam detection mechanisms) designed to identify unsolicited or unwanted emails, including, but not limited to, snowshoeing (i.e., sending spam emails across multiple domains or IP addresses to dilute reputation metrics and evade filters) and waterfalling (i.e., list owner “waterfalls” the same illicitly obtained address list through a series of (usually) unknowing, innocent email service providers. Each time they clean out bounces, complainants and maybe non-respondents, with the end goal being to send the final result through a good email service provider with solid deliverability);
- Disguising, falsifying, or manipulating the subject matter, header, or transmission path information of any email; and
- Conducting security testing, including simulated phishing and other activities that may resemble social engineering or similar attacks.

Deliverability and oneapp Email SaaS Performance Risks

Sending certain emails may result in email deliverability issues or negatively affect the performance of the oneapp Email SaaS or oneapp's business reputation, any one of which may constitute a violation of this Email SaaS Policy, as determined by oneapp, on a case-by-case basis. These include, but are not limited to, sending emails that result in (a) complaints from third parties (e.g., complaints from inbox providers or law enforcement agencies) or an unreasonable number of complaints from recipients (e.g., complaints of spam or similar complaints) or (b) excessive block listings or listings that exceed a reasonable period of time to resolve.

Age Gating

If you are sending emails related to content intended for adults that is not prohibited under this Email SaaS Policy, then you must verify that a recipient is at least of legal age to provide affirmative consent to receive such an email based on where that recipient is located. Upon written request from oneapp, you will provide proof of the age gating mechanisms that are in place.

Creation of Excess Accounts

You are prohibited from creating an excessive number of oneapp Email SaaS accounts for the purposes of circumventing oneapp's internal controls. In general, accounts are limited to one paid oneapp Email SaaS account per customer with the ability to (a) allow multiple users to use the oneapp Email SaaS from a single account and (b) segregate email sending and API activity.

Unauthorized Access and Access Removal

You will use reasonable efforts to (a) prevent unauthorized access to your oneapp Email SaaS account and the oneapp Email SaaS and (b) detect and remove your end users and customers who violate this Email SaaS Policy in connection with their use of the oneapp Email SaaS.