ACCEPTABLE USE POLICY

This acceptable use policy applies to all services that Soprano ("we", "our" or "us") provides to your organisation ("you" or "your").

"Content" means the messages, information, data, text, software, graphics, video or any other materials you store or transmit via our services.

1.1 **COMPLIANCE WITH CONTRACT AND LAW.** When using our services, you must comply with the Services Contract including this Acceptable Use Policy and must not use or permit use of our services for any purpose that would breach applicable law or cause us to do so. Applicable laws will include, without limitation, anti-spam laws, do-not-call laws, and data protection or privacy laws.

1.2 **YOUR RESPONSIBILITY FOR CONTENT.** You are solely responsible for your content and must ensure that you comply with the laws that apply to its transmission. We do not review or provide any editorial or other control over your content.

1.3 **PROHIBITED CONTENT.** Your content must not:

(a) contain material that could reasonably be considered immoral, improper, abusive, deceptive, obscene, defamatory, offensive, discriminatory, malicious or threatening;

(b) promote, assist or incite criminal or illegal activity;

(c) describe or promote explicit sexual activity or violence.

(d) breach the intellectual property rights or other legal rights of third parties;

(e) promote or incite violence, hatred or harm against any person or group, or incite racial hatred;

(f) be false, fraudulent, misleading or deceptive, dishonest or be likely to mislead or deceive (including by impersonating or imitating any person or identity or misrepresenting or obscuring your identity or the source or origin of the content e.g. smishing); or

(g) be illegal, inappropriate or harmful to transmit to, or permit access by minors;

(h) contain sensitive personal information or data, or breach data privacy or privacy laws. (**Note** that RCS messaging does not support end-to-end encryption and although our platform is encrypted and the transit of information across the network to our platform is encrypted, individual messages aren't encrypted and we are not responsible for the security of data once it leaves our (or service provider's) systems to messaging gateways or transmission networks. By using our RBM services, you agree that the RBM service security measures provide a level of security appropriate to the risk in respect of the personal data you transmit, and such transmission is at your election and risk.)

1.4 **PROHIBITED BEHAVIOUR.** You must not use our services:

(a) in a manner that materially interferes with the use of our platform by our other customers, uses any artificial inflation of service or denial of service means, or exceeds the maximum throughput allocated to your identity, or to reverse-engineer or copy any portion of any of our service process, methodology, code or program;

(b) to distribute or use any viruses, trojans, worms or similar malicious code;

(c) to send unsolicited or unwanted or harassing communications (commercial or otherwise) without express consent under applicable law, provided that the foregoing does not exclude the use of two factor authentication or provision of single use passwords with end user consent;

or

(d) in a way that interferes with, degrades or subverts the security or privacy of our services or platform or seeks unauthorized access to computers or networks.

1.5 CONSEQUENCE OF BREACH. Where you breach this policy:

(a) If practical in the circumstances, we will notify you and request that you stop the relevant activity or remove the content; and

(b) If the breach is serious, or if you have not remedied a breach within the reasonable timeframe we have given, we may immediately suspend or terminate our service and delete your content.

Last updated: November 12, 2020.