

Solutions by Text, LLC Acceptable Use Policy **Updated June 5, 2020**

This amended Acceptable Use Policy (“AUP” or “Amended AUP”) replaces the Solutions by Text, LLC (“SBT”) Acceptable Use Policy in effect before June 5, 2020. By beginning or continuing to use SBT’s products and services, Partner consents to be bound by this Acceptable Use Policy.

1.1. Incorporation and Conflict. This AUP represents an integral component of the legally binding Agreement, including all definitions therein, between Solutions by Text, LLC and Partner. This AUP is fully incorporated into the Agreement as if fully set forth therein. If there is a conflict between this AUP and the Agreement, this AUP will govern.

1.2. Scope. Any Partner utilizing the SBT products and services (“SBT Services”) must comply with this AUP. By using or continuing to use SBT’s Services, Partner acknowledges and agrees to ensure compliance with this AUP. This AUP applies to any communication including, but not limited to, Short Message Service (“SMS”) messages, Multimedia Message Service (“MMS”) messages, Rich Communication Service (“RCS”) messages, telephone calls, facsimile transmittals, and email (collectively “Messages”).

1.3. Prohibited Actions. Partner agrees not to use, and, to the extent possible, will discourage its customers (“End Users”) from using, the SBT Services to send Messages containing the following prohibited content:

- (a) junk mail, spam, or unsolicited material to persons or entities that have not agreed to receive such material or to whom Partner or End User do not otherwise have a legal right to send such material;
- (b) material that infringes or violates any third-party’s intellectual property rights, rights of publicity, privacy, or confidentiality, or the rights or legal obligations of any wireless service provider or any of its customers or subscribers;
- (c) material or data that:
 - i. is illegal, harassing, coercive, defamatory, libelous, abusive, threatening, obscene, or otherwise objectionable;
 - ii. is harmful to minors;
 - iii. is excessive in quantity;
 - iv. transmission of which could diminish or harm the reputation or business of SBT, SBT’s Partners, End Users, and/or any third-party service provider involved in the provision and execution of the SBT Services;
 - v. is alcoholic beverage-related (e.g., beer, wine, or liquor), tobacco-related (e.g., cigarettes, cigars, pipes, chewing tobacco), guns or weapons-related (e.g., firearms, bullets), illegal drugs-related (e.g., marijuana, cocaine), pornographic-related (e.g., adult themes, sexual content), crime-related (e.g., organized crime, notorious characters), violence-related or intended to incite violence (e.g., violent games), death-related (e.g., funeral homes, mortuaries), hate-related (e.g. racist organizations), or gambling-related (e.g., casinos, lotteries).
 - vi. has discriminatory or prejudicial content against age, gender, race, ethnicity, country of origin, religion, sexual orientation, disability, geographical location, or any other protected group;

- vii. specifically mentions any wireless carrier or copies or parodies the products or services of any wireless carrier;
- viii. contains viruses, Trojan horses, worms, time bombs, cancelbots, or other computer-programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data, or personal information;
- ix. is false, misleading, or inaccurate;
- x. would expose SBT or any third-party to liability;
- xi. contains any signal or impulse that could cause electrical, magnetic, optical, or other technical harm to SBT or a third-party;
- xii. attempts to find inadequacies, limitations, or vulnerabilities in the SBT API, UI, or Intellectual Property.
- xiii. facilitates a denial of service attack on the SBT API, UI, Intellectual Property, or Services;
- xiv. disrupts or adversely impacts the availability, quality, or stability of the SBT API, UI, Intellectual Property, or Services;
- xv. violates any applicable laws or regulations of any applicable jurisdiction, including, but not limited to: applicable laws or regulations related to the transmission of data, import/export laws, the recording or monitoring of phone calls, and other forms of communication; applicable laws or regulations that prohibit engaging in any unsolicited advertising, marketing, or transmission of communications; applicable anti-spam laws or regulations including, but not limited to, the Canada Anti-Spam Law (“CASL”), the Telephone Consumer Protection Act, the General Data Protection Regulation (“GDPR”), and the Do-Not-Call Implementation Act;
- xvi. transmits unsolicited communications, commercial or otherwise;
- xvii. uses the SBT Services to collect information about individuals without their explicit consent;
- xviii. uses the SBT services to receive or send Protected Health Information (“PHI”) as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), unless the End User has authorized such action in writing;
- xix. records or monitors any communication without consent of all participants; and
- xx. violates any applicable industry standards, policies, or guidelines published by the CTIA (“Cellular Telecommunications Industry Association”), MMA (“Mobile Marketing Association”), or any other recognized entities.

1.4. Restricted Actions. Partner shall not access any SBT Services that Partner has not requested and paid applicable charges for. Partner will not use or attempt to use a third-party’s account with SBT, interfere with the security of or otherwise abuse the SBT Services or SBT’s Partners.

1.5. Notification. Partner is solely responsible for any and all activities that occur within its account with SBT. Partner agrees to immediately notify SBT of any unauthorized use of the SBT Services or any other breach of security or access known to Partner. Partner shall cooperate with SBT in any investigation and other actions taken for suspected or known violations of the AUP, including any incidents caused or suspected to be caused by an End User.

1.6. Sensitive Data. Partner acknowledges that the SBT Services are not to be used in any way to transmit full names, driver’s license numbers, addresses, Social Security numbers, or any other information that is private and sensitive in nature (“Sensitive Data”). SBT strongly advises

against the transmittal by or acceptance of any Sensitive Data in Partner's custody or control. Partner is responsible for ensuring that adequate security measures are in place prior to transmitting Sensitive Data or permitting End Users to transmit Sensitive Data to SBT.

ANY TRANSMISSION OF SENSITIVE DATA TO END USERS THROUGH SBT'S API, UI, INTELLECTUAL PROPERTY, OR SERVICES IS DONE SOLELY AT PARTNER'S RISK. SBT WILL HAVE NO LIABILITY WHATSOEVER IN CONNECTION WITH ANY EVENTS INVOLVING SENSITIVE DATA TRANSMITTED OR PROCESSED VIA SBT'S API, UI, INTELLECTUAL PROPERTY, OR SERVICES UNLESS OTHERWISE PROVIDED IN THE AGREEMENT.

1.7. Updates. SBT may update this AUP upon providing Partner with thirty (30) days' written notice in advance of the updated AUP's effective date ("Effective Date"). The updated AUP will supersede all other versions unless otherwise provided.

1.8. Acceptance. Partner's continued use of SBT Services on or after the updated AUP's Effective Date constitutes Partner's acceptance of the updates provided therein.

1.9. Applicable Law. If changes to the AUP are required by law, mandates from telecommunications providers, or any other necessary requirements that need to be incorporated into the AUP immediately, SBT will not be able to provide thirty (30) days' written notice to Partner. If any changes to the AUP are required immediately, Partner will be notified in writing as soon as commercially reasonable.