ACCEPTABLE USE POLICY

This Acceptable Use Policy ("AUP") governs all uses of Brandlive's services and sites and supplements any Master Services Agreement, Services Agreement, Terms of Service, or other contracting document for the provision and use of Brandlive's services and sites (the "Services Agreement"). This AUP is incorporated by reference into the Services Agreement. Capitalized terms not defined herein have the meaning set forth in the Services Agreement.

Brandlive is committed to providing Services that maintains your trust and confidence. In return, we require that you use the Services responsibly. You will use the Services only for purposes that are legal and proper, in accordance with this AUP. You will use the Services only for business purposes and not for any other purpose. If you become aware of any violations of this AUP, please contact Brandlive at info@brand.live. Brandlive will investigate all reports and take appropriate action (in Brandlive's sole discretion). Brandlive may suspend or terminate Client's use of the Services, any user's access, or the Services Agreement, if Client, any of Client's Authorized Users, or Client's agents or representatives violate this AUP. Client is solely responsible for the data, content, messages, or other information or materials Client, Client's Authorized Users, or Client's agents or representatives transmit, archive, distribute, display, upload, or download through the use or access of the Services. If you cannot comply with this AUP, you may not use the Services.

Prohibited Activities

Client, Client's Authorized Users, or Client's agents or representatives shall not use the Services to:

a) commit a crime, violate any rights of a person or entity (including intellectual property rights), or violate any local, state, national, or international law, rule, or regulation, as applicable;

b) impersonate a person or entity or to otherwise misrepresent any affiliation with a person or entity;

c) commit fraud or make fraudulent offers or advertisements (i.e., make money fast schemes, chain letters, pyramid schemes);

d) transmit harmful or potentially harmful code, including viruses, Trojan horses, worms, time bombs, or any other computer programming routines that could damage, interfere with, surreptitiously intercept, or expropriate any system, program, data, or personal information;

e) transmit bank, credit card, debit card, other card numbers, or other financial account information such as cardholder name, expiration date, PIN or PIN blocks, service code, or track data from a magnetic strip or chip;

f) harvest, collect, or gather user data without consent;

g) act in a way or take any actions that will subject Brandlive to any third-party liability;

h) post, stream, or transmit any content, including live video, that violates this AUP;

i) do anything that threatens, exploits, or otherwise harms children;

j) engage in any activity that is harmful, obscene, or indecent. This includes, for example, displays of nudity, violence, pornography, sexually explicit material, or criminal activity;

k) facilitate or support human trafficking;

l) engage in any activity that supports or facilitates terrorism or terrorist organizations;

m) engage in any activity that is defamatory, harassing, threatening, or abusive;

n) send unauthorized messages, advertising, or spam, including unsolicited promotional or commercial content or other mass solicitation material;

o) violate the privacy of others or distribute confidential or personal information of others;

p) engage in any activity that is harmful or disruptive to the Services or attempts to circumvent restrictions on access, usage, or security of the Services;

q) intercept, monitor, damage, or modify any communication which is not intended for you;

r) gain unauthorized access to any part of the Services, any other user account, computer systems, or networks connected to the Services, through password mining or any other means; or

s) modify, adapt, or create derivative works based upon the Services.

Client shall not (a) reverse engineer any Service; (b) attempt to bypass or break any security mechanism on any of the Services; or (c) use the Services in a manner that poses a security or service risk to Brandlive or other users.

Interference with Services is Prohibited

Client shall not engage in, or attempt to engage in:

a) unauthorized access to or use of the Services, data, or the networks or systems, including an attempt to probe, scan, or overload a Brandlive system or the Services, or to breach security or authentication measures without express written authorization from Brandlive;

b) unauthorized monitoring of code, data, or traffic on a system without express written authorization from Brandlive;

c) deliberate attempts to overload a system and broadcast attacks;

d) an action that imposes an unreasonable or disproportionately large load on Brandlive's infrastructure;

e) performance of a program, script, command, or sending messages of any kind that are designed to interfere with a user's terminal session, by any means, including locally or by the internet;

f) the use of manual or electronic means to avoid any use limitations placed on the Services; or

g) any other activity that could be reasonably interpreted as unauthorized access to or interference with the Services.

Laws Specific to Communications

Clients shall comply with all laws that apply to communications, including wiretapping laws, the Telephone Consumer Protection Act, the Do-Not-Call Implementation Act, CAN-SPAM Act of 2003 and any other laws or regulations applicable to communications, including any third party policies such as the applicable guidelines published by the Cellular Telecommunications Industry Association, the Mobile Marketing Association.

Updates

Brandlive may revise and update this AUP from time to time.

Current Version of AUP: Version 1.1, Effective April 17, 2020.