

BLUSPARK GROUP
ACCEPTABLE USE POLICY
(Effective: [DATE])

Bluspark Global LLC and its subsidiaries and affiliates (“Bluspark,” “we,” or “us”) maintains and offers certain software products to its customers (the “Services”). This Acceptable Use Policy (“AUP”), along with Bluspark’s End User License Agreement (“EULA” located at [____]) governs your access to and use of the Services. You must first read and accept this AUP before accessing the and using the Services. By indicating your acceptance, including your use of any of the Services, you agree to adhere to and be bound by the terms hereof in all respects.

Prohibitions on Use

The prohibitions below have been established by Bluspark to comply with applicable law, ensure reliable service for all of our users, ensure security and privacy of our (and any third party’s) network and systems, maintain Bluspark’s reputation, and preserve the privacy and security of each user at all times.

The Services may only be used for lawful purposes and pursuant to this AUP and the EULA. Additionally, you are prohibited from using the Services as follows:

- In any manner that violates any federal, state, international, or local law or regulation;
- In a manner that materially interferes with our activities or overall business or harms any of our customers, employees, affiliates, agents, officers, or directors;
- To threaten, bypass, or destroy any security mechanism used with or incorporated in the Services;
- To disparage, denigrate, insult, or otherwise make pejorative statements about Bluspark and/or any of its affiliates, directors, officers, employees, partners, brand, products, or service;
- To transmit any content or information that is offensive, lewd, pornographic, defamatory, libelous, harassing, tortious, abusive, illegal, prejudice, discriminatory, or otherwise inappropriate or objectionable;
- To transmit any marketing, advertising or promotional materials, including without limitation any “spam,” “junk mail,” or other deceptive or unsolicited bulk or commercial email;
- To modify, sub-license, adapt, translate, reverse engineer, sell, disassemble, or decompile any portion of the Services or its functionality;
- To impersonate Bluspark (including any Bluspark officer or employee), any user of our website and/or Service, or any other person or entity;
- To transmit any content, data, or material that infringes the intellectual property rights or other personal rights (including privacy) of any third parties;
- To use the Services in connection with unsolicited, unwanted, or harassing communications, including without limitation, SMS messages, phone calls, voice mail, chat, video, or email;
- To transmit any content, data, or material that contains viruses, spyware, spiders, robots, worms, Trojan horses, logic bombs, or any other type of malicious or deleterious programs;
- To use the Services to collect information about other users, including phone numbers or email addresses, without any such individual’s prior explicit consent or otherwise under false pretenses of any kind;
- In any manner that violates any other applicable policy maintained by Bluspark;

- To use the Services to record or monitor a phone call or other communication without first obtaining express consent from the participants per applicable law (such as California’s Invasion of Privacy Act);
- In any manner that can reasonably be considered contrary to Bluspark’s goodwill, public image, and overall reputation;
- To express or imply that any user’s statements, activities, or causes are endorsed by Bluspark;
- To collect, or attempt to collect, personal information about users or other third parties without their prior knowledge and affirmative consent;
- To divulge any of Bluspark’s (or any affiliate’s) proprietary information;
- In any manner that promotes any illegal activity; or
- To knowingly receive, use, re-use, upload or download any material which:
 - Contains material that may reasonably be considered obscene, defamatory, offensive, abusive, hateful, inflammatory, harassing, violent, or otherwise objectionable;
 - Is likely to deceive any person acting reasonably under the circumstances;
 - Impersonates any person; or

Monitoring and Enforcement

Bluspark regularly monitors third-party use of the Services to confirm compliance with the terms of this AUP and any other applicable Bluspark policy. We maintain the right to monitor all such usage by any means we deem appropriate at any time in our sole discretion and delete any material we deem illegal, inappropriate, or violative of any Bluspark or applicable third-party policy. If Bluspark discovers a violation, it will take whatever action it deems reasonably necessary or appropriate to address such behavior. YOU HEREBY WAIVE AND HOLD HARMLESS BLUSPARK, ALONG WITH BLUSPARK’S EMPLOYEES, OFFICERS, DIRECTORS, AFFILIATES, LICENSEES, AND SERVICE PROVIDERS, FROM ANY AND ALL CLAIMS RESULTING FROM, OR ARISING DIRECTLY OR INDIRECTLY OUT OF, ANY ACTION TAKEN BY ANY OF THE FOREGOING PARTIES IN CONNECTION WITH INVESTIGATIONS BY EITHER BLUSPARK OR LAW ENFORCEMENT AUTHORITIES.

Modifications and Updates to this AUP

Bluspark reserves the right to modify and update this AUP at any time in its sole discretion. Except as otherwise provided by Bluspark, updates will be effective upon the date indicated at the top of this AUP. The updated version of the AUP will supersede all prior versions. Note that Bluspark’s failure to enforce this policy in any instance and for whatever reason shall not be construed as a waiver of its right to do so at any other time.

Account Security

Each user is responsible for any misuse of his or her account, even if the inappropriate activity was actually committed by someone other than the account holder (i.e., his or her family member or friend, for example). Therefore, each user must take all reasonable steps to protect his or her account from unauthorized access. In addition, no user may access his or her account to breach the security of any other user’s account or attempt to gain unauthorized access to another server or network. As such, each user must ensure the

security of his or her password at all times, including without limitation, by not sharing it with others for any reason. Additionally, passwords should be hard to guess and changed on a regular basis.

Reporting Violators

Bluspark requests that any user who believes that a violation of this AUP or any other Bluspark policy has taken place should report the alleged violation to Bluspark promptly. The following information should be included:

- Name of alleged violator(s);
- Date and time (including time zone) of the alleged violation(s); and
- Description of alleged violation(s).

The identity of those who report known or suspected violations will be maintained by Bluspark with the utmost secrecy at all times.

If you have any questions regarding this policy, please contact us at [email address].