



ACCEPTABLE USE POLICY

1. **Compliance with Applicable Laws.** Client shall ensure at all times that its use of the Web Services, and any use by its agents or customers, remains in compliance with all applicable law, including without limitation, privacy laws, anticorruption laws, trade sanctions, competition laws, and other legal requirements of the United States, the United Kingdom, and any other jurisdiction in which Client operates, including all legal requirements that may restrict the persons or destinations to which Client may sell its products and services.
2. **Abuse.** Clients will only use the Web Services in a lawful manner that is consistent with this Acceptable Use Policy and the Agreement. The Web Services may not be used to engage in or promote illegal, abusive, deceptive, or irresponsible behavior, including without limitation:
 - a. Distributing, storing, or transmitting any virus or similar content that may be harmful to the Web Services, or to third parties;
 - b. Storing or distributing content that is fraudulent, misleading, or deceptive, or promotes deceptive products or services;
 - c. Allowing unauthorized use of the Web Services to a third party;
 - d. Collecting or using personal data without proper notice and consent;
 - e. Engaging in behavior that is likely to result in retaliation impacting Monetate or the Web Services such as a server being the target of a denial of service attack;
 - f. Monitoring, testing, scanning or crawling the Web Services without first obtaining Kibo's written permission;
 - g. Attempting to interfere with or disrupt the Web Services, for example, by inundating the Web Services with communication requests such that the Web Services are not able to sufficiently respond to legitimate traffic; or
 - h. Renting, leasing, licensing, granting a security interest in, or otherwise transferring or sublicensing Client's rights hereunder to any third party.
3. **E-mail.** Client's use of the Web Services in connection with the delivery of email will be in full compliance with applicable law, including the CAN-SPAM Act of 2003 and Client will not:
 - a. Use any false, misleading or deceptive TCP-IP packet header information in an e-mail or newsgroup posting;
 - b. Defame, libel, slander, impersonate, abuse, harass, threaten, invade the privacy of or otherwise violate or infringe the legal rights (including the rights of privacy and publicity) of any other person;
 - c. Publish, post, distribute, disseminate, advertise or link to any: (i) content, site, topic, name, material or information which is profane, defamatory, libelous, slanderous, infringing, obscene, indecent, or which contains nudity or adult content; (ii) software, content or other material protected by intellectual property laws, copyright licenses, rights of privacy or publicity, or other proprietary rights, unless Client owns or controls such rights or have received all necessary consents for Client's publication, distribution, or linking of such software and other materials; (iii) software, content or other material that contains viruses, worms, corrupted files, cracks or that may or are intended to damage the operation of or render inoperable another's computer, hardware, software, security measures or system or other programs written to defeat the security measures of any computer, system or programs; (iv) software, content, other material or Web site that constitutes "hate speech", whether directed at an individual or a group, and whether based upon the race, sex, creed, national origin, religious affiliation, sexual orientation or language of such individual or group (v) harm minors in any manner;
 - d. Sell, offer to sell, distribute, promote, facilitate, disseminate or link to any sites for marketing, sales, promotion, facilitation or distribution of: illegal gambling; illicit drugs, pharmaceuticals and controlled substances; counterfeit, pirated or stolen goods; any goods or services that infringe or



otherwise violate a third party's rights including copyright, patent, trademark, or rights of publicity or privacy; goods that are considered indecent, obscene or pornographic; registered or unregistered securities; goods or services that Client cannot legally sell; goods which are misrepresented or which do not in fact exist; fraudulent goods; or any other illegal activity.

4. **Large File Content Delivery.** Client agrees not to upload a content file in excess of 20 MB directly to the Web Services. Should Client require the use of content files in excess of 20 MB, Client shall upload such files to its Content Delivery Network, where such files shall be exclusively served from its Content Delivery Network.
5. **Site Traffic Surges.** Client shall provide Monetate with written notice at least thirty (30) days prior to a foreseeable event that is likely to increase traffic by more than ten percent of the average traffic experienced by the Web Services in the thirty days prior to the notice ("Average Traffic"). The notice should provide a brief description of the planned event, including: (i) the expected duration of the event; (ii) the number of web pages that are expected to be affected; and (iii) the expected increase in traffic above Average Traffic. Upon receiving timely notice, Monetate shall provide additional capacity for the event, up to two times the amount it provides for Average Traffic. If Monetate reasonably believes that the event will require more than two times the amount of capacity that it provides for Average Traffic, Monetate shall present Client with a proposed Services Order that sets forth reasonable fees associated with its costs of providing and supporting the additional capacity for the event. If Client fails to provide timely notice or declines such a proposed Service Order for additional capacity, any outage, disruption or unavailability of the Web Services relating to the event will be excluded from calculations of the availability of the Web Services under the Service Level Agreement.
6. **Reporting Violations.** Client will promptly report any known or suspected violations of this Acceptable Use Policy to Monetate in writing. Monetate reserves the right to monitor Client's use of the Web Services to verify compliance. Monetate may take action in response to a violation, as it reasonably determines appropriate, to limit risk or liability. Such action may include blocking access to certain content or suspending access to the Web Services. Monetate will use reasonable efforts to provide Client with notice prior to taking such action.