Acceptable Use Policy

September 19, 2019

This Acceptable Use Policy ("AUP") describes the proper use of the Services and Groups available through Smarsh Central. This AUP is incorporated by reference into the Agreement.

Smarsh may suspend or terminate Client's use of the Services, any User's access to Groups on Smarsh Central, or the Agreement, if Client or any of Clients Users or Representatives violate this AUP. As between Client and Smarsh, Client is solely responsible for the data, content, messages, or other information that Client transmits, archives, distributes, displays, uploads or downloads through its use of the Services.

Prohibited Activities

Client 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 or debit card numbers or 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) create a false identity or forged email address or header, or phone number, or otherwise attempt to mislead others as to the identity of the sender or the origin of a message or phone call;
(g) circumvent another service offered by Smarsh, such as subscribing to email archiving for the purpose of archiving email marketing;
(h) harvest data; or
(i) act in a way that will subject Smarsh to any third-party liability.

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 Smarsh 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 Smarsh system or the Services, or to breach security or authentication measures without express authorization;
(b) unauthorized monitoring of code, data, or traffic on a system without express authorization;
(c) deliberate attempts to overload a system and broadcast attacks;
(d) an action that imposes an unreasonable or disproportionately large load on Smarsh'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, such as timing out; 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.

If Client uses the Services in connection with any bulk and commercial email practices Client shall, in accordance with applicable law:

(a) obtain the verifiable consent of e-mail recipients via affirmative means;
(b) obtain necessary consents in accordance with applicable law;
(c) retain evidence of consents in a form that may be produced on request;
(d) allow a recipient to revoke consent;
(e) post an email address for complaints in a conspicuous place;
(f) have a privacy policy posted for each domain associated with the mailing;
(g) have the means to track anonymous complaints;
(h) not obscure the source of the Client e-mail in any manner; and,
(i) not attempt to send any message to an email address after such number of rejections as is specified by law.

Updates

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

Current Version of AUP: Version 5, Effective September 19, 2019.