Acceptable Use Policy

Data Management Solutions Pty Ltd

This Acceptable Use Policy ("Policy") sets out certain additional obligations of the Customer when using Services under the Data Management Solutions Pty Ltd Customer Agreement. Any capitalized terms not defined in this Acceptable Use Policy have the meaning given to them in the current version of the DMS Customer Agreement.

PART 1 – ACCEPTABLE USE POLICY

1. GENERAL POLICY STATEMENT

1.1. The Customer must not (and must ensure that any person using the Services (User) does not) use or attempt to use the Services in any manner that violates:
1.1.1. any applicable local, state, federal or international law (including, without limitation, the Spam Act 2003 (Cth) (Spam Act) and the Copyright Act (1968 (Cth)); or
1.1.2. the rights of any third party (including, without limitation, infringement of copyright, trademark, or other intellectual property right, misappropriation of trade secrets, electronic fraud, invasion of privacy, pornography, obscenity and libel).
1.2. The Customer must not (and must ensure that any User does not) in the course of using the Services engage or attempt to engage in any activities that:
1.2.1. interfere with or disrupt other Network users, Network services or Network equipment;
1.2.2. involve the unauthorized use of any machine or network, denial of service attacks, falsifying header information or user identification information, monitoring or scanning the networks of others;
1.2.3. introduce or allow the introduction of any virus, worm, trojan horse, zombie, key logger or other malicious code into the Services or any Network; or
1.2.4. are fraudulent, misleading or intended to mislead.
1.3. For the purpose of clause 1.2, interference or disruption includes, without limitation, distribution of unsolicited advertising or chain letters, repeated harassment of other Network users, impersonating another such user, falsifying one's network identity for improper or illegal purposes, sending unsolicited bulk emails or calls, continuing to send someone emails after being asked to stop, propagation of computer worms and viruses, mail bombing and "flashing" and using a Network to gain unauthorized entry to any other machine accessible via a Network.
1.4. The customer must (and must ensure that any User does not) engage or attempt to engage in any abusive, rude or unacceptable communications with any Ninefold employee, officer or agent.

2. SPAM

2.1. In this clause, “spam” includes one or more unsolicited commercial electronic messages with an Australian link for purposes of the Spam Act, and derivations of the word “spam” have corresponding meanings.
2.2. The Customer may not use the Service to:
2.2.1. send, allow to be sent, or assist in the sending of spam;
2.2.2. use or distribute any software designed to harvest email addresses; or
2.2.3. otherwise breach the Spam Act or the Spam Regulations 2004 (Cth) or any applicable local, state, federal or international law.
2.3. DMS may suspend the Services in the following circumstances:
2.3.1. if the Services are being used to host any device or service that allows emails to be sent between third parties not under the Customer’s authority and control; or
2.3.2. if the Customer or any User is in breach of clause 2.2, provided however that Ninefold will first make reasonable attempts to contact the Customer and give the Customer the opportunity to address the problem within a reasonable time period (having regard to the severity of the problems being caused by the open service or breach referred to above).
2.4. In accordance with its responsibilities under the Spam Act and the Internet Industry Association Spam Code (Spam Code) or any applicable local, state, federal or international law or code, DMS may:
2.4.1. restrict the Customer’s ability to forward emails;
2.4.2. limit the Customer’s access to the Service to a closed user group relevant to its use of the Service;
2.4.3. require the Customer to take all necessary actions to comply with, or which assist Ninefold to comply with, the Spam Act or the Spam Code or any applicable local, state, federal or international law or code.

3. CONTENT PUBLISHING

3.1. The Customer must not publish material that is or would be classified by the Classification Board or similar body as RC or X rated via websites, email, newsgroups or other publishing media accessible via the Services.
3.2. The Customer must take appropriate precautions to prevent minors from accessing or receiving any content the Customer has published that may be inappropriate for them. This includes implementing a restricted access system on content that is or would be classified by the Classification Board as R rated.

4. BREACH OF THIS POLICY

4.1. If the Customer or any User uses the Service in a way that DMS, in its absolute discretion, believes breaches this Policy, DMS may take any action it deems appropriate to respond to such a breach.
4.2. Actions that DMS may take pursuant to clause 4.1 include (but are not limited to):
4.2.1. temporary or permanent removal of content and content publishing capabilities;

4.2.2. filtering of Internet transmissions;
4.2.3. immediate suspension or termination of all or any part of the Services;
4.2.4. gather information from the Users involved and the complaining party, if any, and examine transmissions and material on its servers and any Network;
4.2.5. cooperate with law enforcement authorities in the investigation of suspected criminal violations and the system administrators at Providers or any other service provider.
4.3. DMS may by notice to the Customer elect to give the Customer 24 hours (or such longer period as reasonably necessary and specified in the notice) to remedy any breach of this Policy, before taking any action pursuant to clause 4.2.
4.4. DMS is not obligated to monitor the Customer's or any User's use of the Services (including any content posted, disseminated or accessed by the Customer or any User), but reserves the right to do so in order to:
4.4.1. investigate any suspected breach of this Policy;
4.4.2. enforce this Policy;
4.4.3. protect any other Network users, Network services or Network equipment;
4.4.4. cooperate with law enforcement authorities in the investigation of suspected criminal violations and the system administrators at Providers or any other service provider. Such cooperation may include DMS providing the username, IP address or other identifying information about a User; and
4.4.5. comply with any applicable laws or regulations.
4.5. Ninefold reserves the right to charge the Customer, on a time and materials basis, for any costs (including labor costs) incurred by DMS as a result of or arising from any breach of this Policy by the Customer or any User. The Customer is liable for any charges invoiced in accordance with this clause.

5. AMENDMENT

This Policy may be amended by DMS at any time by posting an amended version on our website. The amended policy will apply once posted on our website. By continuing to use the Services on or after the amended policy has been posted, the Customer will be deemed to have accepted and agreed to be bound by the Policy as amended.

PART 2 – DEFINITIONS

In this Policy:

Customer means the person, company or other legal entity who has agreed to be bound by the DMS Customer Agreement.

Emergency means a situation that, unless immediately remedied, the potential to jeopardize human life or safety or to cause immediate risk to property.

Network has the same meaning as “Telecommunications Network” in the Telecommunications Act 1997 (Cth) and definitions used in this act have the same meaning unless the contrary intention otherwise appears.

Services means the services described in the DMS Customer Agreement.

Premises means a building, structure or vessel owned, occupied or used by the Customer facility, or to which a Service is supplied or at which any of the Customer’s or a Provider’s property is located.

Provider means a carrier, service provider or other supplier used by DMS to supply the Services or Equipment to the Customer.

Revised October 2013