Acceptable Use Policy

This Acceptable Use Policy ("AUP") applies to Customer, and its end users or any third party that uses the network, internet and hosting services (“Subscribers”) provided by NTT United Kingdom Limited (“NTT UK”) and sets out the activities that are not permitted on networks and infrastructure owned or operated by NTT UK or its affiliates worldwide.

Subscribers shall not:

a) send unsolicited bulk and/or commercial messages over the Internet (known as "spamming"). It is not only harmful because of its negative impact on consumer attitudes toward NTT UK, but also because it can overload NTT UK's network and disrupt service to NTT UK Subscribers.

b) maintain an open SMTP relay.

c) engage in any activity that infringes or misappropriates the intellectual property rights of a third party, including copyrights, trademarks, service marks, trade secrets, software piracy, and patents held by individuals, corporations, or other entities. Nor shall Subscribers engage in any activity that violates privacy, publicity, or other personal rights of others.

d) use the NTT UK network to advertise, transmit, store, post, display, or otherwise make available child pornography or obscene speech or material. NTT UK is required by law to notify law enforcement agencies when it becomes aware of the presence of child pornography on, or being transmitted through, NTT UK's network.

e) use NTT UK's network as a means to transmit or post defamatory, harassing, abusive, or threatening language.

f) forge or misrepresent message headers, whether in whole or in part, to mask the originator of the message.

g) access illegally or without authorisation computers, accounts, or networks belonging to another party, or attempt to penetrate security measures of another individual's system (often known as "hacking"); nor conduct any activity that might be used as a precursor to an attempted system penetration (i.e. port scan, stealth scan, or other information gathering activity).

h) distribute information regarding the creation of and sending of internet viruses, worms, Trojan horses, pinging, flooding, mail bombing, or denial of service attacks (DoS); nor conduct any activities that disrupt the use of or interfere with the ability of others to effectively use the network or any connected network, system, service, or equipment.

i) advertise, transmit, or otherwise make available any software, program, product, or service that is designed to violate this AUP, which includes the facilitation of the means to spam, initiation of pinging, flooding, mail bombing, denial of service attacks, and piracy of software.

j) export encryption software over the internet or otherwise, to points outside the Subscriber’s country which is contrary to that respective country's rules and regulations.

k) engage in activities that are or are likely to be in breach of any applicable laws, or be determined to be illegal, including advertising, transmitting, or otherwise making available ponzi schemes, pyramid schemes, fraudulently charging credit cards, and pirating software.

l) engage in activities, whether lawful or unlawful, that NTT UK determines to be harmful to its Subscribers, operations, reputation, goodwill, or customer relations.

m) engage in any gambling activity in violation of any required licenses, codes of practice, or necessary technical standards required under the laws or regulations of any jurisdiction in which Subscriber's site is hosted or accessed.

The responsibility for avoiding the harmful activities described above rests primarily with the Subscribers. NTT UK will not, as an ordinary practice, monitor the communications of its Subscribers to ensure that they comply with NTT UK policy or applicable law.

Should NTT UK become aware of harmful activities, however, it may take any action to stop the harmful activity, including but not limited to, removing information, shutting down a web site, implementing screening software designed to block offending transmissions, denying access to the internet, or take any other action it deems appropriate.

NTT UK will not intentionally monitor private electronic mail messages sent or received by its Subscribers unless required to do so by law, governmental authority, or when public safety is at stake. NTT UK may, however, monitor its service electronically to determine that its facilities are operating satisfactorily. Also, NTT UK may disclose information, including but not limited to, information concerning a Subscriber, a transmission made using our network, or a web site, in order to comply with a court order, subpoena, summons, discovery request, warrant, statute, regulation, or governmental request. If NTT UK is legally required to permit a relevant authority to inspect Subscriber's content or traffic, NTT UK will give Subscriber reasonable prior notice of such requirement where legally permissible.

NTT UK may disclose Subscriber information or information transmitted over its network where necessary to protect NTT UK and others from harm, or where such disclosure is necessary to the proper operation of the system.

We hope this AUP is helpful in clarifying the obligations of Subscribers, as responsible members of the Services.

Customer must immediately notify NTT UK of any unauthorized access or attempted breach of security and may report violations of this AUP or make any complaints via email to abuse@eu.ntt.net.