MindFireInc℠
Marketing's Missing Link.℠
2601 Main Street, Suite 830
Irvine, CA 92614
Toll Free: (877) 560-3473
Fax: (949) 474-5967
http://www.MindFireInc.com

Electronic Communications Acceptable Use Policy

Effective: August 10, 2021

1. Purpose

The purpose of this Acceptable Use Policy ("AUP") is to ensure the proper and fair use of Mindfire Internet Solutions, Inc.'s ("Mindfire") communications networks, including, without limitation, Electronic Mail and Short Message Service aka Text Messaging (SMS) (collectively, "Electronic Communication(s)"). This AUP is incorporated by reference into any definitive agreement between the user and Mindfire ("Agreement"). Capitalized terms not defined in this AUP will have the meanings set forth in the Agreement. This AUP may be amended at any time and such amendment or termination will be effective at the time Mindfire posts the revised AUP to its website(s).

ANY DIRECT, INDIRECT OR ATTEMPTED VIOLATIONS OF THE AUP SHALL BE CONSIDERED A MATERIAL BREACH OF THE POLICY AND THE SERVICES MAY, AT MINDFIRE'S SOLE DISCRETION, AND ABSENT PRIOR NOTICE, BE IMMEDIATELY TERMINATED, SUSPENDED, CONDITIONED, RESTRICTED OR MODIFIED.

2. Policy

2.1. General

All use of Electronic Communications must be consistent with Mindfire's policies and procedures of ethical conduct and safety and be in compliance with applicable laws and proper business practices. The prohibited uses described in this AUP are intended as minimum guidelines regarding improper and inappropriate conduct and should not be interpreted as an exhaustive list.

Mindfire's Electronic Communication infrastructure should be used primarily for business-related purposes associated with Mindfire's applications. Use of Electronic Communications in order to promote any competitor of Mindfire is strictly prohibited.

Mindfire's Electronic Communication systems shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disability, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
Any recipient of Electronic Communication generated from use of Mindfire's applications with such prohibitive content should immediately report the matter to Mindfire at compliance@mindfireinc.com.

2.2. Communications Compliance

Mindfire and its third-party service providers reserve the right to: (i) monitor any and all communications transmitted through their communication platforms; (ii) disclose any information transmitted through such networks as may be deemed necessary to comply with any law, regulation and/or policy; and/or (iii) remove or refuse to post any materials they determine to be unacceptable, offensive, undesirable, in violation of the law or this AUP. As such, Mindfire may monitor Electronic Communications without prior notice, and contact individuals for compliance related directives. However, Mindfire has no obligation to monitor each Electronic Communication sent through its systems.

Further, any by use of Mindfire's systems, platforms and/or applications, both Mindfire and its third-party service providers are granted the right to access, copy and transmit copies of the content from electronic mail campaigns for the purpose of developing tools and systems to effectively monitor and control abuses.

2.3. Legal Compliance

Electronic Communications must be consistent with Mindfire's policies and procedures of ethical conduct, safety and be compliant with applicable laws, regulations and proper business practices, including, without limitation, to CAN-SPAM (The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003), CASL (Canadian Anti-Spam Law), E-Privacy Directive from the European Union, the Telephone Consumer Protection Act (TCPA), and the Children's Online Privacy Protection Act. For SMS, the messages must comply with rules and regulations established by Common Short Code Administration (CSCA).

2.4. Requirements; Restrictions; Prohibited Uses

2.4.1. Electronic Communications must meet the following requirements: (i) may not contain any false, misleading or deceptive information in its content or header, and may not attempt to obscure or hide the source of the message; (ii) must not be characteristic of spam as determined by the sole discretion of Mindfire; (iv) Electronic Communications in the European Union (EU) and/or sent to or received by EU Residents must comply with GDPR by getting consent from the recipients outlining permissible purpose for such

communications; and (v) Mindfire's services, applications and platforms can only be used for the approved permissible purpose under GDPR.

Mindfire's network or distribution systems may not be used to publish, transmit or store any content or links that: (i) constitutes, depicts, fosters, promotes or relates in any manner to unlawful, illegal, threatening, harassing, abusive, libelous, defamatory, obscene, offensive, indecent, pornographic, sexually explicit, profane, or otherwise objectionable information of any kind, including, without limitation, any transmissions constituting or encouraging conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any laws; (ii) is excessively violent, incites violence, threatens violence, or contains hate speech; (iii) creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement; (iv) is associated with terrorism; (v) exposes trade secrets or other confidential or proprietary information of another person without explicit permission; (vi) infringes on another person's copyright, trade or service mark, patent, or other intellectual property rights; (vii) promotes illegal drugs, illegal arms trafficking or violates export laws; (viii) is illegal or solicits conduct that is illegal under applicable laws; and (ix) is false, malicious or fraudulent, as determined by the sole discretion of Mindfire.

2.4.2. Mindfire's infrastructure must may not be used to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including, but not limited to: (i) interference with service to any user or network including for purposes such as mail bombing, flooding, deliberate attempts to overload a system, and/or transmitting computer viruses and Trojan horses; (ii) collecting or using email addresses, mobile phone numbers, screen names, or other personal identifiers and related information without the consent of the person identified or the owner of the information; (iii) probing, scanning, penetrating, reverse-engineering or testing the vulnerability of Mindfire's network, service, system or device to breach, attempt to breach or collect information about security or authentication measures, or any similar or related activity, without Mindfire's express written consent; (iv) any conduct that causes or is likely to result in retaliation against Mindfire's network, website, employees, officers or other agents, including engaging in behavior that results in any server being the target of a Distributed Denial of Service (DDoS) attack; and/or (v) any conduct that is deemed abusive, malicious or harmful as determined at the sole discretion of Mindfire.

2.4.3. In order to protect the integrity of its network and to achieve the highest rates of deliverability for all of its customers, Mindfire prohibits use of Electronic Communications to otherwise promote and/or transmit any of the following content: (i) payday loans (short term unsecured loans); (ii) debt collection; (iii) debt consolidation and reduction; (iv) credit repair; (v) tax relief programs; (vi) online gambling; (vii) Ponzi, "get rich quick," pyramid schemes or similar speculative investment opportunities; (viii) work from home or make money online opportunities; or (ix) day trading or penny stocks.

2.4.4. Mindfire may, at its sole discretion, choose to temporarily suspend designated services in the event use of the causes a high volume of traffic disrupting the normal system performance, including, for instance, Distributed Denial of Services (DDoS).

2.4.5. Mindfire may restrict, suspend or ban the use of the shared IP pools or otherwise employ any mitigating remedy in the event that spam or any other complaints result from utilization of its services. However, Mindfire may offer the opportunity to utilize and pay for a dedicated IP service in such instance.

2.4.6. Mindfire's systems, platforms and applications are not designed, intended, or authorized for use in any mission critical, emergency, life-saving or life sustaining systems, or for any other application in which the failure of the service could lead to personal injury or death, or to physical or environmental damage.

2.5. Bulk or Commercial Electronic Communications

Bulk or commercial Electronic Communications are defined as any message for which the primary purpose is the advertisement or promotion of a commercial product, website, or service. Such communications must adhere to the following: (i) must not send Electronic Communications to lists that have been purchased from a third-party; (ii) the intended recipients must have given their consent to receive such Electronic Communications specifically from the sender and, for EU, the required consent cannot be based on pre-ticked boxes or default opt-in selection and has to be an explicit opt-in or written consent compliant with GDPR; (iii) procedures for seeking consent include reasonable means to ensure that the person giving consent is the owner of the email address or mobile phone number for which consent is given; (iv) proof of each recipient's consent must be retained in a form that can be promptly produced on request and such, at minimum, must also contain the date, time and method of obtaining the consent; (v) procedures must be in place that allow a recipient to revoke their consent – such as an industry standard unsubscribe link in the body of the email, or sending a STOP message to a SMS sender. The sender must honor revocations of consent and notify the recipient within 48 hours. Further, opting in to a specific mobile marketing program does not give permission to be sent messages from any other campaign not specifically related to that program. For EU applicable territories and users, the sender will also honor the right to be forgotten under GDPR; (vi) sender must have a Privacy Policy posted for its users; (vii) Electronic Communications must not generate excessive "blacklistings" or any critical blacklisting as determined at the sole discretion of Mindfire; (viii) Electronic Communications must not generate excessive spam complaints as determined at the sole discretion of Mindfire; and (ix) Electronic Communications lists must contain valid addresses/contact numbers and must not generate excessive failures or hard bounces as determined at the sole discretion of Mindfire.

3. Security and Encryption

This section applies only to emails sent from Mindfire's systems and not SMS.

Users may only send email originating from a domain address that is registered to the user, is under the user's control, or that the user has received permission to transmit from on behalf-of the owners of the domain.

In order to secure the domain associated with the “From Email Address” of the emails, the domain(s) must be identified by using a Sender Policy Framework (SPF) record in the Domain Name Service (DNS) of the particular domain.

Mindfire recommends digitally signing every email being sent using Domain Key Identification (DKIM)so as to facilitate a more secure delivery. Mindfire’s premium email service sends all emails using TLS encryption if the receiving mail server supports it. The premium email service is available as a standard on Mindfire’s and as an upgrade on Mindfire’s LWC product.

Notwithstanding the foregoing, Electronic Communications services provided by Mindfire and/or its third-party agents should not be considered a "secure communications medium" for any purpose whatsoever and no expectation of privacy is afforded or guaranteed.