

## Acceptable Use Policy

Last Modified January 19, 2023

As a provider of Internet access, web site hosting, and other Internet related services, Grafton Technologies, Inc. ("GTI") offers it's customers, their customers, and end-users (collectively known as "Subscribers"), the means to acquire and disseminate a wealth of public, private, commercial, and noncommercial information. GTI respects that the Internet provides a forum for free and open discussion and dissemination of information, however, when there are competing interests at issue, GTI reserves the right to take certain preventative or corrective actions. In order to protect these competing interests, GTI has developed an Acceptable Use Policy ("AUP"), which supplements and explains certain terms of each customer's respective service agreement and is intended as a guide to the customer's rights and obligations when utilizing GTI's services. This AUP will be revised from time to time. A customer's use of GTI's services after changes to the AUP are posted on GTI's web site, [www.gtec.com](http://www.gtec.com), will constitute the customer's acceptance of any new or additional terms of the AUP that result from those changes.

One important aspect of the Internet is that no one party owns or controls it. This fact accounts for much of the Internet's openness and value, but it also places a high premium on the judgment and responsibility of those who use the Internet, both in the information they acquire and in the information they disseminate to others. When Subscribers obtain information through the Internet, they must keep in mind that GTI cannot monitor, verify, warrant, or vouch for the accuracy and quality of the information that Subscribers may acquire. For this reason, the Subscriber must exercise his or her best judgment in relying on information obtained from the Internet, and also should be aware that some material posted to the Internet is sexually explicit or otherwise offensive. Because GTI cannot monitor or censor the Internet, and will not attempt to do so, GTI cannot accept any responsibility for injury to it's Subscribers that results from inaccurate, unsuitable, offensive, or illegal Internet communications. Subscribers use GTI's resources when accessing the Internet. This includes, but is not limited to, resources like IP addresses, transport facilities, and CPE equipment. Subscribers will receive one IP address and one connection to the Internet, except where additional resources are requested and paid for. Subscribers are prohibited from redistributing GTI's services for any reason unless permission has been granted in writing by GTI.

When Subscribers disseminate information through the Internet, they also must keep in mind that GTI does not review, edit, censor, or take responsibility for any information it's Subscribers may create. When Subscribers place information on the Internet, they have the same liability as other authors for copyright infringement, defamation, and other harmful speech. Also, because the information they create is carried over GTI's network and may reach a large number of people, including both Subscribers and non-subscribers of GTI, Subscribers' postings to the Internet may affect other Subscribers and may harm GTI's goodwill, business reputation, and operations. For these reasons, Subscribers violate GTI policy and the service agreement when they, their customers, affiliates, or subsidiaries engage in the following prohibited activities or any other activity determined by GTI to be unacceptable.:

**SPAMing** – Sending unsolicited, bulk and/or commercial messages over the Internet (known as "SPAMing"). It is not only harmful because of it's negative impact on consumer attitudes toward GTI, but also because it can overload GTI's network and disrupt service to GTI Subscribers. Also, maintaining an open SMTP relay is prohibited. When a complaint is received, GTI has the discretion to determine from all of the evidence whether the email recipients were from a "Confirmed Opt-in" email list. With Confirmed Opt-in (also called Closed-Loop Opt-in) the email recipient has verifiable confirmed permission (also known as "Verifiable Confirmation Information") for the address to be included on the specific mailing list, by confirming (responding to) the list subscription request verification. This is the standard practice for all responsible Internet mailing lists, as it ensures users are properly subscribed, from a working address, and with the address owner's consent. GTI

reserves the right to request from Subscriber the Verifiable Confirmation Information and to verify this information with the email recipient. Further, SPAM does not have to be sent from the Subscriber account or GTI's network to violate GTI policy. Email sent by or through a third party that advertises or otherwise directs traffic or links to the Subscriber web site or Subscriber account will be held to the same standard as those emails sent directly by Subscriber. The use of email lists obtained or purchased from a third party must also be verifiable by Subscriber to meet the requirements of Confirmed Opt-in with Verifiable Confirmation Information that recipient has opted-in to email from Subscriber.

**Intellectual Property Violations** – Engaging in any activity that infringes or misappropriates the intellectual property rights of others, including but not limited to copyrights, trademarks, service marks, trade secrets, software piracy, and patents held by individuals, corporations, or other entities. Also, engaging in activity that violates privacy, publicity, or other personal rights of others. GTI is required by law to remove or block access to customer content upon receipt of a proper notice of copyright infringement. It is also GTI's policy to terminate the privileges of customers who commit repeat violations of copyright laws.

**Child Pornography** – Using GTI's network to advertise, transmit, store, post, display, or otherwise make available child pornography. GTI has a no tolerance policy for child pornography, and accounts reported to GTI as potentially containing child pornography will be immediately disabled and reported to the NCMEC. GTI is required by law to notify law enforcement agencies when it becomes aware of the presence of child pornography on or being transmitted through GTI's network.

**Defamatory or Abusive Language** - Using GTI's network as a means to transmit or post defamatory, harassing, abusive, or threatening language.

**Forging of Headers** – Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message.

**Illegal or Unauthorized Access to Other Computers or Networks** – Accessing illegally or without authorization computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "Hacking"). Also, 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).  
**Security Scans** – GTI understands the needs of our Subscribers to meet certain industry requirements that require Subscriber or a third party engaged by Subscriber to conduct security scans of the Subscriber account or web site. All such scans must be coordinated in advance with GTI. Requirements for conducting any scan on GTI's network can be obtained from [info@gtec.net](mailto:info@gtec.net). Failure to coordinate and meet all requirements prior to scanning is a violation of GTI policy.

**Distribution of Internet Viruses, Worms, Trojan Horses, or Other Destructive Activities** – Distributing information regarding the creation of and sending Internet viruses, worms, Trojan horses, ping, flooding, mailbombing, or denial of service attacks. Also, 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.  
**Facilitating a Violation of this AUP** – Advertising, transmitting, or otherwise making 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 ping, flooding, mailbombing, denial of service attacks, and piracy of software among other malicious activities. This can include failure to update software used on Subscriber account or web site that is known to be vulnerable to malicious activity or exploitation. GTI also expects Subscriber to use secure passwords to protect Subscriber account and associated email accounts. Use of passwords deemed by GTI to be insecure are a violation of GTI policy.

**Export Control Violations** – Exporting encryption software over the Internet or otherwise, to points outside the

United States.

**Usenet Groups** – GTI reserves the right not to accept postings from newsgroups where we have actual knowledge that the content of the newsgroup violates the AUP.

**Other Illegal Activities** – Engaging in activities that are determined to be illegal, including advertising, transmitting, or otherwise making available ponzi schemes, pyramid schemes, fraudulently charging credit cards, and pirating software.

**Other Activities** – Engaging in any activity, whether lawful or unlawful, that GTI determines to be harmful to GTI, it's Subscribers, operations, reputation, goodwill, or customer relations. As we have pointed out, the responsibility for avoiding the harmful activities just described rests primarily with the Subscriber. GTI will not, as an ordinary practice, monitor the communications or content of it's Subscribers to ensure that they comply with GTI policy or applicable law. When GTI becomes 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.

GTI also is aware that some of it's Subscribers are, themselves, providers of Internet services, and that information reaching GTI's facilities from those Subscribers may have originated from a customer of the Subscriber or from another third party. GTI does not require it's Subscribers who offer Internet services to monitor or censor transmissions or web sites created by customers of it's Subscribers.

GTI has the right to directly take action against a customer of a Subscriber. Also, GTI may take action against the Subscriber because of activities of a customer of the Subscriber, even though the action may effect other customers of the Subscriber. Similarly, GTI expects that Subscribers who offer Internet services will cooperate with GTI in any corrective or preventive action that GTI deems necessary.

Failure to cooperate with such corrective or preventive measures is a violation of GTI policy. GTI expects that it's Subscribers who provide Internet services to others will comply fully with all applicable laws concerning the privacy of online communications. A Subscriber's failure to comply with those laws will violate GTI policy. GTI also is concerned with the privacy of online communications and web sites. In general, the Internet is neither more nor less secure than other means of communication, including mail, facsimile, and voice telephone service, all of which can be intercepted and otherwise compromised. As a matter of prudence, however, GTI urges it's Subscribers to assume that all of their online communications are insecure.

GTI cannot take any responsibility for the security of information transmitted over GTI's facilities. GTI will not intentionally monitor private electronic mail messages, or other forms of communication, sent or received by it's Subscribers unless required to do so by law, governmental authority, or when public safety is at stake. GTI may, however, monitor it's service electronically to determine that it's facilities are operating satisfactorily. Also, GTI 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. GTI assumes no obligation to inform the Subscriber that Subscriber information has been provided and in some cases may be prohibited by law from giving such notice.

Finally, GTI may disclose Subscriber information or information transmitted over it's network where necessary to protect GTI and others from harm, or where such disclosure is necessary to the proper operation of the system. Finally, GTI wishes to emphasize that by choosing to use the service, Subscribers indemnify GTI for any violation of any service agreement, law, policy, or this AUP that results in loss to GTI or the bringing of any claim

against GTI by any third party. This means that if GTI is sued because of a Subscriber's or customer of a Subscriber's activity, the Subscriber will pay any damages awarded against GTI, plus costs and reasonable attorneys' fees. The Subscriber or customer of a Subscriber may be held liable for any service outage relating to improper use of GTI services, including but not limited to SPAMing, port probing, DOS attacks, virus infection, etc. Also, GTI reserves the right to charge a fee to reinstate or reconnect a customer that has been disconnected or suspended due to violation of this or any other GTI policy.

We hope this AUP is helpful in clarifying the obligations of Internet users, including GTI and its Subscribers, as responsible members of the Internet. Any complaints about a Subscriber's violation of this AUP should be sent to [info@gtec.net](mailto:info@gtec.net). Use of the Services constitutes acceptance of our Privacy Policy, in which we may, from time to time, test your broadband service to be sure we're offering the best service, as may be required by Federal Communications Commission requirements.