HCTC Network Management & Acceptable Use Policy

I. General Matters

Why is HCTC providing this Policy to me?

This Network Management and Acceptable Use Policy (the "Policy") describes HCTC's policies and protocol in providing all HCTC Internet services (the "Service") and outlines your acceptable use of the Service. This Policy is in addition to any restrictions contained in the HCTC Internet Communications Service Agreement (the "Subscriber Agreement") available on our website.

What obligations do I have under this Policy?

Everyone who uses the Service must comply with this Policy. Failure to comply with this Policy could result in the suspension or termination of your Service account. If you do not agree to comply with this Policy, you must immediately stop all use of the Service and notify HCTC so it can close your account.

How will I know when HCTC changes this Policy?

HCTC may revise this Policy from time to time by posting a new version on the Web site at http://www.hctc.net or any successor URL(s) (the "HCTC Internet Web Site"). HCTC will use reasonable efforts to make customers aware of any changes to this Policy, which may include sending email announcements or posting information on the HCTC Internet Web Site. Revised versions of this Policy are effective immediately upon posting. You should conform your use of the Service to the most recent version of the Policy and pay attention when you are notified of changes.

Where do I send questions about or report violations of the Policy?

Questions concerning this Policy and reports of violations of it may be sent at http://hctc.net/contact-us/. To report illegal content on the Internet go to www.fcc.gov. Child exploitation or other incidents involving the Internet which violate criminal laws should be reported to law enforcement authorities at http://www.justice.gov/criminal/ceos/.

II. Prohibited Uses and Activities Prohibited Uses and Activities

What uses and activities does HCTC prohibit?

In general, the Policy prohibits uses and activities involving the Service that are illegal, infringe the rights of others, or interfere with or diminish the use and enjoyment of the Service by others. For example, these prohibited uses and activities include, but are not limited to, using the Service, Customer Equipment, or any HCTC provided equipment, either individually or in combination with another, to:

Conduct and information restrictions:

- Undertake or accomplish any unlawful purpose. This includes, but is not limited to, posting, storing, transmitting or disseminating information, data or material which is libelous, obscene, unlawful, threatening or defamatory, or which infringes the intellectual property rights of any person or entity, or which in any way constitutes or encourages conduct that would constitute a criminal offense, or otherwise violate any local, state, federal, or non-U.S. law, order, or regulation.
- Post, store, send, transmit, or disseminate any information or material which a reasonable person could deem to be unlawful.
- Upload, post, publish, transmit, reproduce, create derivative works of, or distribute in any way information, software or other material obtained through the Service or otherwise that is protected by copyright or other proprietary right, without obtaining any required permission of the owner.
- Transmit unsolicited bulk or commercial messages, commonly known as "spam."

- Send very large numbers of copies of the same or substantially similar messages, empty messages, or messages which contain no substantive content, or send very large messages or files that disrupts a server, account, blog, newsgroup, chat, or similar service.
- Initiate, perpetuate, or in any way participate in any pyramid or other illegal scheme.
- Participate in the collection of very large numbers of email addresses, screen names, or other identifiers of others (without their prior consent), a practice sometimes known as spidering or harvesting, or participate in the use of software (including "spyware") designed to facilitate this activity.
- Collect responses from unsolicited bulk messages.
- Falsify, alter, or remove message headers.
- Falsify references to HCTC or its network, by name or other identifier, in messages.
- Impersonate any person or entity, engage in sender address falsification, forge anyone else's digital or manual signature, or perform any other similar fraudulent activity (for example, "phishing").
- Violate the rules, regulations, terms of service, or policies applicable to any network, server, computer database, service, application, system, or Web site that you access or use.

Technical restrictions:
- Use the Service or facilities for web-hosting, e-mail hosting, or other unusually high-bandwidth consumption unless you have made special subscription arrangements with HCTC and the usage does not otherwise violate law or regulation.
- Access any other person's computer or computer system, network, software, or data without his or her knowledge and consent; breach the security of another user or system; or attempt to circumvent the user authentication or security of any host, network, or account. This includes, but is not limited to, accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other hosts, networks, or accounts without express permission to do so.
- Use or distribute tools or devices designed or used for compromising security or whose use is otherwise unauthorized, such as password guessing programs, decoders, password gatherers, keystroke loggers, analyzers, cracking tools, packet sniffers, encryption circumvention devices, or Trojan Horse programs. Unauthorized port scanning is strictly prohibited.
- Copy, distribute, or sublicense any proprietary software provided in connection with the Service by HCTC or any third party, except that you may make one copy of each software program for back-up purposes only.
- Distribute programs that make unauthorized changes to software (cracks).
- Use or run dedicated, stand-alone equipment or servers from the location to which HCTC provides your services (the "Premises") that provide network content or any other services to anyone outside of your Premises local area network ("Premises LAN"), also commonly referred to as public services or servers. Examples of prohibited equipment and servers include, but are not limited to, email, Web hosting, file sharing, and proxy services and servers.
- Use or run programs from the Premises that provide network content or any other services to anyone outside of your Premises LAN, except for personal and non-commercial residential use.
- Service, alter, modify, or tamper with any equipment provided to you by HCTC in connection with the provision of the Service ("HCTC Equipment") or permit any other person to do so who is not authorized by HCTC.

Network and usage restrictions:
- Restrict, inhibit, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the Service (except for tools for safety and security functions such as parental controls, for example), including, without limitation, posting or transmitting any information or software which contains a worm, virus, or other harmful feature, or generating levels of traffic sufficient to impede others' ability to use, send, or retrieve information
- Restrict, inhibit, interfere with, or otherwise disrupt or cause a performance degradation, regardless of intent, purpose or knowledge, to the Service or any HCTC (or HCTC supplier) host, server, backbone network, node or service, or otherwise cause a performance degradation to any facilities used by HCTC to deliver the Service

P.O. Box 768 • Ingram, Texas 78025 • Toll Free 800.292.5457 • Fax 830.367.5993 • hctc.net
This institution is an equal opportunity provider and employer.
Version: March 2018

2 of 6

- Resell the Service or otherwise make available to anyone outside the Premises the ability to use the Service (for example, through Wi-Fi or other methods of networking), in whole or in part, directly or indirectly. The Service is for personal use by the subscriber only and you agree not to use the Service for operation as an Internet service provider or for any business enterprise or purpose (whether or not for profit)
- HCTC reserves the right to suspend or terminate Service accounts where data consumption is not characteristic of a typical user of the Service subscribed to as determined by HCTC in its sole discretion
- Connect the HCTC Equipment to any computer outside of your Premises
- Interfere with computer networking or telecommunications service to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abusing operator privileges, and attempts to "crash" a host
- Accessing and using the Service with anything other than a dynamic Internet Protocol ("IP") address that adheres to the dynamic host configuration protocol ("DHCP"). You may not configure the Service or any related equipment to access or use a static IP address or use any protocol other than DHCP unless you are subject to a Service plan that expressly permits you to do so
- HCTC conducts several security initiatives, and offers security tools for our customers at www.hctc.net.

III. Customer Conduct and Features of the Service

What obligations do I have under this Policy?

In addition to being responsible for your own compliance with this Policy, you are also responsible for any use or misuse of the Service that violates this Policy, even if it was committed by a friend, family member, or guest with access to your Service account. Therefore, you must take steps to ensure that others do not use your account to gain unauthorized access to the Service by, for example, strictly maintaining the confidentiality of your Service login and password. In all cases, you are solely responsible for the security of any device you choose to connect to the Service, including any data stored or shared on that device. HCTC recommends against enabling file or printer sharing unless you do so in strict compliance with all security recommendations and features provided by the manufacturer of the applicable file or printer sharing devices. Any files or devices you choose to make available for shared access on a home LAN, for example, should be protected with a strong password or as otherwise appropriate.

It is your responsibility to secure your data and your equipment which connects to the Service from external threats such as viruses, spam, bot nets, and other methods of intrusion.

How does HCTC address inappropriate content and transmissions?

HCTC reserves the right to refuse to transmit or post, and to remove or block, any information or materials, in whole or in part, that it, in its sole discretion, deems to be in violation of Sections II or III of this Policy, which are transmitted to or placed upon a system within HCTC's control e.g. HCTC's website or sites hosted by HCTC. Absent special circumstances, such as requests from law enforcement, HCTC has no right to and does not monitor content merely transmitted by its Service or initiated by or stored on your system. However, HCTC and its affiliates, suppliers, and agents have the right to monitor transmissions which violate this Policy which HCTC, in its reasonable discretion, believes violate this Policy or could be otherwise harmful to HCTC's network or customers using the Service, e.g. spam, malware, suspicious addresses, etc., and to block or remove them in accordance with this Policy, the Subscriber Agreement, and applicable law.

What requirements apply to electronic mail?

The Service may not be used to communicate or distribute email or other forms of communications in violation of Section II of this Policy. As described below in Section IV of this Policy, HCTC uses reasonable network management tools and techniques to protect customers from receiving spam and from sending spam (often without their knowledge over an infected computer).

P.O. Box 768 • Ingram, Texas 78025 • Toll Free 800.292.5457 • Fax 830.367.5993 • hctc.net
This institution is an equal opportunity provider and employer.
Version: March 2018
3 of 6

HCTC is not responsible for deleting or forwarding any email sent to the wrong email address by you or by someone else trying to send email to you. HCTC is also not responsible for forwarding email sent to any account that has been suspended or terminated. This email will be returned to the sender, ignored, deleted, or stored temporarily at HCTC's sole discretion. In the event that HCTC believes in its sole discretion that any subscriber name, account name, or email address (collectively, an "identifier") on the Service may be used for, or is being used for, any misleading, fraudulent, or other improper or illegal purpose, HCTC (i) reserves the right to block access to and prevent the use of any of these identifiers and (ii) may at any time require any customer to change his or her identifier. In addition, HCTC may at any time reserve any identifiers on the Service for HCTC's own purposes. In the event that a Service account is terminated for any reason, all email associated with that account (and any secondary accounts) will be permanently deleted as well.

HCTC Internet email has a 30 MB message size limit with a limit at 150 recipients per email.

What requirements apply to instant, video, and audio messages?
Each user is responsible for the contents of his or her instant, video, and audio messages and the consequences of any of these messages. HCTC assumes no responsibility for the timeliness, mis-delivery, deletion, or failure to store these messages. In the event that a Service account is terminated for any reason, all instant, video, and audio messages associated with that account (and any secondary accounts) would be permanently deleted as well.

Does HCTC employ network security practices in addition to the congestion management technique?
Yes. As described above, HCTC employs a number of practices to help prevent unwanted communications such as spam as well as protect the security of our customers and network. HCTC limits the number of login, SMTP, DNS, and DHCP transactions per second (at levels far above 'normal' rates) that customers can send to HCTC's servers in order to protect them against Denial of Service (DoS) attacks. We do not disclose the exact rate limits in order to maintain the effectiveness of these measures, which ensure that these critical services are available for all of our customers.

IV. Network Management and Limitations on Data Consumption

What are HCTC's practices concerning net neutrality in its network management?
- Transparency: The commercial terms for HCTC internet accounts can be found at www.hctc.net.
- No Blocking and No Unreasonable Discrimination: HCTC does not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management. HCTC does not unreasonably discriminate in transmitting lawful network traffic over its broadband internet access service.
- Reasonable Network Management: HCTC's data network has redundant data backbone facilities and equipment that instantaneously re-routes traffic in the event of a cable cut or other outage. We monitor our network's performance around the clock. We measure capacity utilization at each routing and switching node within our network. When peak utilization consistently exceeds 75% of capacity at a node, HCTC will analyze overall network consumption and may augment capacity to prevent customers from experiencing blockages. Although we do not dedicate capacity to individual customers utilizing our mass-market Internet access products, as that would be highly inefficient, we manage our data network capacity to avoid blockages. Because our network design and build strategy is aimed at avoiding blockages, it is unnecessary to have data traffic management policies for those rare instances when peak utilization exceeds capacity.

Does HCTC discriminate against particular types of online content?
No. HCTC provides its customers with full access to all the lawful content, services, and applications that the Internet has to offer.

Why does HCTC manage its network?
HCTC manages its network with one goal: to deliver the best possible broadband Internet experience to all of its customers. High-speed bandwidth and network resources are not unlimited. Managing the network is essential to promote the use and enjoyment of the Internet by all of our customers. We use reasonable network management

P.O. Box 768 • Ingram, Texas 78025 • Toll Free 800.292.5457 • Fax 830.367.5993 • hctc.net
This institution is an equal opportunity provider and employer.
Version: March 2018

4 of 6

practices that are consistent with industry standards. We also try to use tools and technologies that are minimally intrusive. Just as the Internet continues to change and evolve, so too will our network management practices as we seek to address the challenges and threats on the Internet.

All Internet service providers need to manage their networks and HCTC is no different. In fact, many of them use the same or similar tools that HCTC does. If we didn't manage our network, our customers would be subject to the negative effects of spam, viruses, security attacks, network congestion, and other risks and degradations of the service. By engaging in reasonable and responsible network management, HCTC can deliver the best possible broadband Internet experience to all of its customers.

Does HCTC block P2P traffic or applications like BitTorrent, Gnutella, or others?
No. HCTC does not block P2P traffic or applications like BitTorrent, Gnutella, or others as part of its current network congestion management technique. HCTC does not manage congestion based on the applications being used by customers, nor does it manage type of content that is generating traffic congestion. Accordingly, customer traffic is congestion managed not based on the applications or content being used but based on current network conditions and recent amounts of data transferred by users.

How does HCTC manage its network?
HCTC uses various tools and techniques in managing its network, delivering the Service, and ensuring compliance with this Policy and the Subscriber Agreement. These tools and techniques are dynamic, like the network and its usage, and can and do change frequently. For example, these network management activities may include (i) identifying spam and preventing its delivery to customer email accounts, (ii) detecting malicious Internet traffic and preventing the distribution of viruses or other harmful code or content, (iii) temporarily lowering the priority of traffic for users who are the top contributors to current network congestion, and (iv) using other tools and techniques that HCTC may be required to implement in order to meet its goal of delivering the best possible Internet experience to all of its customers.

Are there restrictions on data consumption that apply to the Service?
You must ensure that your use of the Service does not restrict, inhibit, interfere with, or degrade any other person's use of the Service, nor represent (as determined by HCTC in its sole discretion) an overly large burden on the network. In addition, you must ensure that your use of the Service does not limit or interfere with HCTC's ability to deliver and monitor the Service or any part of its network. If you use the Service in violation of the restrictions referenced above, that is a violation of this Policy. In these cases, HCTC may, in its sole discretion, suspend or terminate your Service account or request that you subscribe to a version of the Service (such as a commercial grade Internet service, if appropriate) if you wish to continue to use the Service at higher data consumption levels. HCTC may also provide versions of the Service with different speed and data consumption limitations, among other characteristics, subject to applicable Service plans. HCTC's determination of the data consumption for Service accounts is final.

<div align="center">

V. Violation of this Acceptable Use Policy

</div>

What happens if you violate this Policy?
HCTC reserves the right immediately to suspend or terminate your Service account and terminate the Subscriber Agreement if you violate the terms of this Policy or the Subscriber Agreement.

How does HCTC enforce this Policy?
HCTC does not routinely monitor the activity of individual Service accounts for violations of this Policy. However, in the company's efforts to promote good citizenship within the Internet community, it will respond appropriately if it becomes aware of inappropriate use of the Service. HCTC has no obligation to monitor the Service and/or the network. However, HCTC reserves the right at any time to monitor bandwidth, usage, transmissions, and content in order to,

P.O. Box 768 • Ingram, Texas 78025 • Toll Free 800.292.5457 • Fax 830.367.5993 • hctc.net
This institution is an equal opportunity provider and employer.
Version: March 2018

5 of 6

among other things, operate the Service; identify violations of this Policy; and/or protect the network, the Service and HCTC users.

HCTC prefers to inform customers of inappropriate activities and give them a reasonable period of time in which to take corrective action. HCTC also prefers to have customers directly resolve any disputes or disagreements they may have with others, whether customers or not, without HCTC's intervention. However, if the Service is used in a way that HCTC or its suppliers, in their sole discretion, believe violates this Policy, HCTC or its suppliers may take any responsive actions they deem appropriate under the circumstances, with or without notice. Neither HCTC nor its affiliates, suppliers, or agents will have any liability for any of these responsive actions. These actions are not HCTC's exclusive remedies and HCTC may take any other legal or technical actions it deems appropriate with or without notice.

HCTC reserves the right to investigate suspected violations of this Policy, including the gathering of information from the user or users involved and the complaining party, if any, and examination of material on HCTC's servers and network. During an investigation, HCTC may suspend the account or accounts involved and/or remove or block material that potentially violates this Policy. You expressly authorize and consent to HCTC and its suppliers cooperating with (i) law enforcement authorities in the investigation of suspected legal violations, and (ii) and system administrators at other Internet service providers or other network or computing facilities in order to enforce this Policy. Upon termination of your Service account, HCTC is authorized to delete any files, programs, data, email and other messages associated with your account (and any secondary accounts).

The failure of HCTC or its suppliers to enforce this Policy, for whatever reason, shall not be construed as a waiver of any right to do so at any time. You agree that if any portion of this Policy is held invalid or unenforceable, that portion will be construed consistent with applicable law as nearly as possible, and the remaining portions will remain in full force and effect. You agree to indemnify, defend and hold harmless HCTC and its affiliates, suppliers, and agents against all claims and expenses (including reasonable attorney fees) resulting from any violation of this Policy. Your indemnification obligation will survive any termination of the Subscriber Agreement.

How can I contact HCTC if I have any questions about network management?
Go to the page at www.hctc.net for more information about contacting HCTC Internet Customer Service.

P.O. Box 768 • Ingram, Texas 78025 • Toll Free 800.292.5457 • Fax 830.367.5993 • hctc.net
This institution is an equal opportunity provider and employer.
Version: March 2018

6 of 6