



Stowe Access, LLC  
Stowe Cablevision, Inc.  
Jeffersonville Cable TV  
Stowe VOIP, LLC

## STOWE ACCESS AND JEFFERSONVILLE ACCESS ACCEPTABLE USE POLICY FOR RESIDENTIAL HIGH-SPEED INTERNET SERVICE

### Contents

1. [Prohibited Uses and Activities](#)
2. [Customer Conduct and Features of the Service](#)
3. [Network Management and Limitations on Data Consumption](#)
4. [Violation of this Acceptable Use Policy](#)
5. [Copyright and Digital Millennium Copyright Act Requirements](#)

### Why is Access providing this Policy to me?

Access goal is to provide its customers with the best residential cable internet service possible. In order to help accomplish this, Access has adopted this Acceptable Use policy (the "Policy"). This Policy outlines acceptable use of the Access High-Speed Internet service (the "Service"). This Policy is in addition to any restrictions contained in the Access Agreement for Residential Services (the "Subscriber Agreement") available at [Stoweaccess.com](http://Stoweaccess.com).

### What obligations do I have under this Policy?

All Access High-Speed Internet customers and all others who use the Service (the "Customer," "user," "you," or "your") must comply with this Policy. Your 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 Access so that it can close your account.

### How will I know when Access changes this Policy and how do report violations of it?

Access may revise this Policy from time to time by posting a new version on the Web site at [www.stoweaccess.com](http://www.stoweaccess.com). Access will use reasonable efforts to make customers aware of any changes to this Policy, which may include posting information on the [stoweaccess.com](http://stoweaccess.com) Web site. Revised versions of this Policy are effective immediately upon posting. Accordingly, customers of the Access High-Speed Internet Service should read any Access announcements they receive and regularly visit the [stoweaccess.com](http://stoweaccess.com) Web site and review this Policy to ensure that their activities conform to the most recent version.

## 1. Prohibited Uses and Activities

### What uses and activities does Access 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 the Access Equipment, either individually or in combination with one another, to:

### Conduct and information restrictions

This includes, but is not limited to, posting, storing, transmitting or dissemination 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 is 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, reproduce, 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 e-mail 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 Access 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**

Access and 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 Access 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 Premises that provide network content or any other services to any outside of your Premises local area network ("Premises LAN"), also commonly referred to as public services or servers. Examples of prohibited equipment and servers included, but are not limited to, e-mail, 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 the Access Equipment or Service or permit any other person to do the same who is not authorized by Access;

## **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 Access (or Access supplier) host, server, backbone network, node or service, or otherwise cause a performance degradation to any Access (or Access supplier) facilities used to deliver the Service;

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 and non-commercial residential use only and you agree not use the Service for operation as an Internet service provider or for any business enterprise or purpose (whether or not for profit);

Connect the Access Equipment to any computer outside of your Premises;

Interfere with computer networking or telecommunications serve to any user, host or network, including, without limitation, denial of service attack, flooding of a network, overloading a service, improper seizing and abusing operator privileges, and attempts to "crash" a host; and

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 an protocol other than DHCP unless you are subject to a Service plan that expressly permits you to do so.

## **2. 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 the Service, including any data stored or shared on that device. Access recommends against enabling file or printer sharing unless you do so in strict compliance with all security recommendations and features provided by Access and 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 also your responsibility to secure the Customer Equipment and any other Premises equipment or programs not provided by Access that connect to the Service from external threats such as viruses, spam, bot nets, and other methods of intrusion.

### **How does Access address inappropriate content and transmission?**

Access 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 1 or 2 of this Policy, or otherwise harmful to Access network or customers using the Service, regardless of whether this material or its dissemination is unlawful so long as it violates this Policy. Neither Access nor any of its affiliates, suppliers, or agents have any obligation to monitor transmissions or postings (including, but not limited to , email, file transfer, blog, newsgroup, and instant message transmissions as well as materials available on the Personal Web Pages on Online Storage features) made on the Service. However, Access and its affiliates, suppliers, and agents have the right to monitor these transmissions and postings from

time to time for violations of this Policy and to disclose, 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 e-mail or other forms of communications in violation of Section 1 of this Policy. As described below in Section 3 of this Policy, Access 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).

Access is not responsible for deleting or forwarding any e-mail sent to the wrong e-mail address by you or by someone else trying to send e-mail to you. Access is also not responsible for forwarding e-mail sent to any account that has been suspended or terminated. This e-mail will be returned to the sender, ignored, deleted, or stored temporarily at Access sole discretion. In the event that Access believes in its sole discretion that any subscriber name, account name, or e-mail 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, Access (1) reserves the right to block access to and prevent the use of any of these identifiers and (2) may at any time require any customer to change his or her identifier.

In addition, Access may at any time reserve any identifiers on the Service for Access own purposes. In the event that a Service account is terminated for any reason, all e-mail associated with that account (and any secondary accounts) will be permanently deleted as well.

#### **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. Access 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) will be permanently deleted as well.

### **3. Network Management and Limitations on Data Consumption**

#### **Why does Access manage its network?**

Access 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 as Access works to promote the use and enjoyment of the Internet by all of its customers. The company uses reasonable network management practices that are consistent with industry standards. Access tries to use tools and technologies that are minimally intrusive and, in its independent judgment guided by industry experience, among the best in class. Of course, the company’s network management practices will change and evolve along with the uses of the Internet and the challenges and threats on the Internet.

The need to engage in network management is not limited to Access. In fact, all Internet service providers manage their networks. Many of them use the same or similar tools that Access does. If the company didn’t manage its network, its customers would be subject to the negative effects of spam, viruses, security attacks, network congestion, and other risks and degradations of service. By engaging in responsible network management including enforcement of this Policy, Access can deliver the best possible broadband Internet experience to all of its customers.

#### **How does Assess manage its network?**

Access uses various tools and techniques to manage its network, deliver the Service, and ensure 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 (1) identifying spam and preventing its delivery to customer e-mail account, (2) detecting malicious Internet traffic and preventing the distribution of viruses or other harmful code or content, (3) temporarily lowering the priority of traffic for users who are the top

contributors to current network congestion, and (4) using other tools and techniques that Access may be required to implement in order to meet its goal of delivering the best possible broadband Internet experience to all of its customers.

#### **Are there restrictions on data consumption that apply to the Service?**

The Service is for personal and non-commercial residential use only. Therefore, Access reserves the right to suspend or terminate Service accounts where data consumption is not characteristic of a typical residential user of the Service as determined by the company in its sole discretion. Access has established a monthly data consumption threshold per Access High-Speed Internet account of up to 3 Mbps down / 768 Kbps up. Enhanced internet up to 12 Mbps down / 2 Mbps up. Common activities that may cause excessive data consumption in violation of this Policy include, but are not limited to, numerous or continuous bulk transfers of files and other high capacity traffic using (1) file transfer protocol ("FTP"), (2) peer-to-peer applications, and (3) newsgroups. You must also 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 Access 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 Access 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, Access 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. Access may also provide versions of the Service with different speed and data consumption limitations, among other characteristics, subject to applicable Service plans. Access determination of the data consumption for Service accounts is final.

#### **4. Violation of this Acceptable Use Policy**

##### **What happens if you violate this Policy?**

Access 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 Access enforce this Policy?**

Access does not routinely monitor the activity of individual Service accounts for violations of this Policy, except for determining aggregate data consumption in connection with the data consumption provisions 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. Access has no obligation to monitor the Service and/or the network. However, Access and its underlying providers reserve the right at any time to monitor bandwidth, usage, transmissions, and content in order to, among other things, operate the Service; identify violations of this Policy; and/or protect the network, the Service and Access users.

Access prefers to inform customers of inappropriate activities and give them a reasonable period of time in which to take corrective action. Access also prefers to have customers directly resolve any disputes or disagreements they may have with others, whether customers or not, without Access intervention. However, if the Service is used in a way that Access or its underlying providers, in their sole discretion, believe violates this Policy, Access or its suppliers may take any responsive actions they deem appropriate under the circumstances with or without notice. These actions include, but are not limited to, temporary or permanent removal of content, cancellation of newsgroup posts, filtering of Internet transmissions, and the immediate suspension or termination of all or any portion of the Service (including but not limited to newsgroups). Neither Access nor its affiliates, suppliers, or agents will have any liability for any of these responsive actions. These actions are not Access exclusive remedies and Access may take any other legal or technical actions it deems appropriate with or without notice.

Access 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 Access servers and network.

During an investigation, Access may suspend the account or accounts involved and/or remove or block material that potentially violates this Policy. You expressly authorize and consent to Access and its underlying providers cooperating with (1) law enforcement authorities in the investigation of suspected legal violations, and (2) 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, Access is authorized to delete any files, programs, data, e-mail and other messages associated with your account (and any secondary accounts).

The failure of Access or its underlying providers 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 Access and its underlying providers, and agents against all claims and expenses (including reasonable attorney fees) resulting from any violation of this Policy. Your indemnification will survive any termination of the Subscriber Agreement.

## **5. Copyright and Digital Millennium Copyright Act Requirements**

### **Requirements**

#### **What is Access DMCA policy?**

Access is committed to complying with U.S. copyright and related laws, and requires all customers and users of the Service to comply with these laws. Accordingly, you may not store any material or content on, or disseminate any material or content over, the Service (or any part of the Service) in any manner that constitutes an infringement of third party intellectual property rights, including rights granted by U.S. copyright law. Owners of copyrighted works who believe that their rights under U.S. copyright law have been infringed may take advantage of certain provisions of the Digital Millennium Copyright Act of 1998 (the "DMCA") to report alleged infringements. It is Access policy in accordance with the DMCA and other applicable laws to reserve the right to terminate the Service provided to any customer or user who is either found to infringe third party copyright or other intellectual property rights, including repeat infringers, or who Access, in its sole discretion, believes is infringing these rights. Access may terminate the Service at any time with or without notice for any affected customer or user.

#### **How do copyright owners report alleged infringements to Access?**

Copyright owners may report alleged infringements of their works that are stored on the Service or the Personal Web Features by sending Access authorized agent a notification of claimed infringement that satisfies the requirements of the DMCA. Upon Access receipt of a satisfactory notice of claimed infringement for these works, Access will respond expeditiously to either directly or indirectly (1) remove the allegedly infringing work(s) stored on the Service or the Personal Web Features or (2) disable access to the work(s). Access will also notify the affected customer or user of the Service of the removal or disabling of access to the work(s).

Copyright owners may send Access a notification of claimed infringement to report alleged infringements of their works to:

Stowe Access, LLC  
172 Thomas Lane  
Stowe, VT 05672  
Phone: 802-253-9282  
Fax: 802-253-7812  
Email: [stoweaccess@stoweaccess.com](mailto:stoweaccess@stoweaccess.com)

Copyright owners may use their own notification of claimed infringement form that satisfies the requirements of Section 512(c)(3) of the U.S. Copyright Act. Under the DMCA, anyone who knowingly makes misrepresentations regarding alleged copyright infringement may be liable to Access, the alleged infringer, and the affected copyright owner for any damages incurred in connection with the removal, blocking, or replacement of allegedly infringing material.

**What can customers do if they receive a notification of alleged infringement?**

If you receive a notification of alleged infringement as described above, and you believe in good faith that the allegedly infringing works have been removed or blocked by mistake or misidentification, then you may send a counter notification to Access. Upon Access receipt of a counter notification that satisfies the requirements of DMCA, Access will provide a copy of the counter notification to the person who sent the original notification of claimed infringement and will follow the DMCA's procedures with respect to a received counter notification. In all events, you expressly agree that Access will not be a party to any disputes or lawsuits regarding alleged copyright infringement.

If a notification of claimed infringement has been filed against you, you can file a counter notification with Access designated agent using the contact information shown above. All counter notifications must satisfy the requirements of Section 512(g)(3) of the U.S. Copyright Act.

*Revised and effective: August 1, 2011*