VYVE BROADBAND ACCEPTABLE USE POLICY

Updated April 2021

Why is the Company providing this Policy to me?

Our goal is to provide customers with the best residential cable Internet service possible. In order to help accomplish this goal, we have adopted this Acceptable Use Policy (this "Policy"). This Policy outlines acceptable use of our residential high-speed Internet service (the "Service"). This Policy is in addition to any restrictions or conditions contained in the Company's Residential Services Subscriber Agreement (the "Subscriber Agreement") and DMCA Policy, respectively available on our website at http://www.vyvebroadband.com/policies. All capitalized terms used in this Policy that are not defined herein shall have the meanings given to them in the Subscriber Agreement.

All residential Internet customers (the "customer," "user," "you," or "your") and all others who use the Service must comply with this Policy. Your failure, or others' failure, to comply with this Policy could result in the suspension or termination of your or their Service accounts. Therefore, you should take steps to ensure that others you permit to use your Service are aware of this Policy and agree to abide by it. If you are unwilling to comply with this Policy, you must immediately stop all use of the Service and notify the Company so that we can close your account.

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

The Company may revise this Policy from time to time by posting a new version on our web site at http://vyvebroadband.com/policies. The Company will use reasonable efforts to make customers aware of any changes to this Policy, which may include sending email announcements or posting information on our website. Revised versions of this Policy are effective immediately upon posting. Accordingly, customers of the Service should read any announcements they receive from the Company and regularly visit our website and review this Policy to ensure that their activities conform to the most recent version.

I. PROHIBITED USES AND ACTIVITIES

What uses and activities does the Company prohibit?

The Service may only be used for lawful purposes. Transmission or distribution of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret, or other intellectual property right used without proper authorization, and material that is obscene, illegal, defamatory, constitutes an illegal threat or violates export control laws. Your use of the Service is also subject to the Company's DMCA Policy available on our website at https://vyvebroadband.com/wp-content/uploads/Vyve-DMCA-Policy_August2017.pdf and https://www.yournorthland.com/legal/copyright/ for customers served by our Northland subsidiaries.

Any activity or use of the Service which violates system network security or integrity is prohibited and may result in civil or criminal liability. In general, this 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. These prohibited uses and activities include, but are not limited to, using the Service, Customer Equipment, or Company Equipment, either individually or in combination with one another, to:

Conduct and Information Restrictions

- undertake or accomplish any unlawful purpose (including, but 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 disrupt 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 the Company 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 website that you access or use;

Technical Restrictions

- 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 (including, but 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 us or any third party, except that you may make one copy of each software program for backup purposes only;

- distribute programs that make unauthorized changes to software (“cracks”);

- use or run dedicated, stand-alone equipment, servers or programs from 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, except for personal and non-commercial residential use. Examples of prohibited equipment and servers include, but are not limited to, email, web hosting, file sharing, and proxy services and servers;

- service, alter, modify, or tamper with the Company Equipment or Service or permit any other person to do the same who is not authorized by us;

Network and Usage Restrictions

- use the Service for any purpose other than personal and non-commercial residential use (except for your individual use for telecommuting);

- use the Service for operation as an Internet service provider or for any business, other legal entity, or organization purpose (whether or not for profit);

- restrict, inhibit, or otherwise interfere, regardless of intent, purpose or knowledge, with the ability of any other person 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 contain a worm, virus, or other harmful feature;

- 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 Company host, server, backbone network, node or service, or otherwise cause a performance degradation to any Company facilities used to deliver the Service;

- resell the Service or otherwise make available to anyone outside of your Premises the ability to use the Service (for example, through WiFi or other methods of networking), in whole or in part, directly or indirectly, with the sole exception of your use of Company-provided Internet Service in accordance with its then-current terms and policies, which you will protect with an appropriate password;

- connect the Company 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; or

- access and use 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.

II.CUSTOMER CONDUCT AND FEATURES OF THE SERVICE

What obligations do I have under this Policy?

You are responsible for your own compliance with this Policy. You are also responsible for any use or misuse of the Service that violates this Policy by anyone else you permit to access the Service (such as a friend, family member, or guest), with one exception: in cases where you permit others to access your Company-provided Internet Service with their own login information, those users are responsible for complying with all then-current terms and policies that apply to their access.

We recommend against enabling file or printer sharing unless you do so in strict compliance with all security recommendations and features provided by Company 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.

In all cases, you are solely responsible for the security of any device you connect to the Service, including any data stored or shared on that device. It is also your responsibility to secure the Customer Equipment and any other Premises equipment or programs not provided by Company

that connect to the Service from external threats such as viruses, spam, bot nets, and other methods of intrusion.

How does the Company address inappropriate content and transmissions?

We reserve the right to refuse to transmit or post, and to remove or block, any information or materials, in whole or in part, that we, in our sole discretion, deem to be in violation of this Policy or otherwise harmful to our network or customers using the Service, regardless of whether this material or its dissemination is unlawful, so long as it violates this Policy. Neither the Company 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 Features (as defined below)) made on the Service. However, the Company 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 email or other forms of communication in violation of this Policy. As described below in Section III of this Policy, we use reasonable network management tools and techniques to protect customers from receiving spam and from sending spam (often without their knowledge over an infected computer).

We are 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. We are 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 our sole discretion. If you cancel or terminate your Service account for any reason, all email associated with that account (and any secondary accounts) will be permanently deleted as well.

If we believe, in our 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, we (i) reserve 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, we may at any time reserve any identifiers on the Service for our own purposes.

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. We assume no responsibility for the timeliness, misdelivery, deletion, or failure to store these messages. If you cancel or terminate your Service account for any reason, all instant, video, and audio messages associated with that account (and any secondary accounts) will be permanently deleted as well.

What requirements apply to personal web pages and file storage?

As part of the Service, we provide access to personal web pages and storage space through personal web pages and online storage features (collectively, the "Personal Web Features"). You are solely responsible for any information that you or others publish or store on the Personal Web Features. You are also responsible for ensuring that all content made available through the Personal Web Features is appropriate for those who may have access to it. For example, you must take appropriate precautions to prevent minors from receiving or accessing inappropriate content. We reserve the right to remove, block, or refuse to post or store any information or materials, in whole or in part, that we, in our sole discretion, deem to be in violation of this Policy. For purposes of this Policy, "material" refers to all forms of communications including text, graphics (including photographs, illustrations, images, drawings, logos), executable programs and scripts, video recordings, and audio recordings. We may remove or block content contained on your Personal Web Features and terminate your Personal Web Features and/or your use of the Service if we determine that you have violated the terms of this Policy. The Company assumes no obligation to back up or retain any information that you or others store or maintain on the Personal Web Features and we reserve the right to delete all such information upon termination of the Service.

III.NETWORK MANAGEMENT

Why do we manage our network?

We manage our network with one goal: to deliver the best possible broadband Internet experience to all of our customers. High-speed bandwidth and network resources are not unlimited. Managing the network is essential as we work to promote the use and enjoyment of the Internet by all of our customers. We use reasonable network management practices that are consistent with industry standards and aim to use tools and technologies that are minimally intrusive in order to protect our customers from the negative effects of spam, viruses, security attacks, network congestion, and other risks and degradations of service. By engaging in legally permitted and responsible network management practices, including enforcement of this Policy, we can deliver the best possible broadband Internet experience to all of our customers. You can review our Network Management Disclosure policy at http://www.vyvebroadband.com/policies.

How does Company manage its network?

We use various tools and techniques to manage our 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 (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, and (iii) using other tools and techniques that may be required to meet our goal of delivering the best possible broadband Internet experience to all of our customers.

IV. DATA CONSUMPTION

What data consumption requirements apply to the Service?

In certain locations we are providing the Service with different speed thresholds, among other characteristics, subject to applicable Service plans. You can learn about the Service plans that apply in your area by going to http://www.vyvebroadband.com. If we change this approach, we will post a new version of this Policy as described above and make other appropriate notifications to customers.

In addition, except for our "Unlimited" Plan, in all locations the Service is subject to a monthly data usage allowance. **Our "Unlimited" Plan is intended for residential customers and typical personal use. If you exceed four (4) terabytes of data monthly, a Company customer service agent may contact you to discuss a commercial data plan option or, if you fail to take such a plan, we may reduce your data speed to 10 Mbps until the next billing cycle.** For Internet Service plans other than our "Unlimited" Plan and pre-paid plans (which are described below), if you have provided us with your email address, we will send an email to that address if and when you reach 75%, 90% and 100% of your plan's monthly data usage allowance. We will also send a session interrupt message to the MAC ID on your account when you reach 75%, 90% and 100% of your plan's monthly data usage allowance in a particular calendar month. You are solely responsible for providing a correct email address to us and for assuring that messages from us arenot filtered into a spam folder. See http://www.vyvebroadband.com/home/mydatameter for more information on the data usage allowance applicable to your Service plan and how you can monitor, manage and make the most of your online data usage. Should you exceed the monthly data usage allowance for your plan in a particular calendar month, you will still enjoy the same speed and access, but will be charged an additional $10 per month for every additional increment of 50 GB or portion thereof of data used. You also have the option to purchase an additional 250GB of data upfront for $25 in order to avoid or minimize overage charges. If you find that you are regularly exceeding the data usage allowance applicable to your service plan, please contact a customer service representative at 1.855.FOR.VYVE to discuss alternatives. Our customer service representativesare trained to help customers explore options to reduce data consumption.

Unused data from your monthly data allowance expires at the end of each month and does not carry over to subsequent months.

In certain regions, in addition to our standard plans, we offer thirty-day pre-paid plans for Internet Service which vary depending on the speed and data allowance offered. We may limit a customer to subscription to one of our pre-paid plans in certain circumstances, including, without limitation, if the customer has past due payments or does not pay a requested deposit. If you subscribe to one of these plans, your Internet Service will remain active for thirty days or until you reach the applicable data allowance purchased, whichever occurs first. For pre-paid plans, if you have provided us with your email address, we will send an email to that address if and when you reach 50%, 75%, 90% and 100% of your plan's monthly data usage allowance. We will also send a session interrupt message to the MAC ID on your account when you reach 50%, 75%, 90% and 100% of your plan's monthly data usage allowance. You are solely responsible for providing a correct email address to us and for assuring that messages from us are not filtered into a spam folder.

Unused data from your pre-paid data allowance expires at the end of your billing cycle and does not carry over to subsequent billing cycles.

V. VIOLATION OF THIS ACCEPTABLE USE POLICY

What happens if you violate this Policy?

We reserve the right to immediately suspend or terminate your Service account and terminate the Subscriber Agreement if you violate the terms of this Policy or the Subscriber Agreement, or if anyone else you permit to access the Service violates this Policy. Depending upon the extent of any violation of these acceptable use restrictions, Customers may receive warnings or, in some cases, have their accounts suspended. We reserve the right to monitor Customers' actions when deemed necessary to troubleshoot connectivity problems or determine if there is an abuse. In our sole discretion, the Company may initiate an investigation and, in order to prevent further possible unauthorized activity, may suspend access to Service. Confirmation of violations may result in termination of Service and criminal prosecution.

How do we enforce this Policy?

We do not routinely monitor the activity of individual Service accounts for violations of this Policy, except for determining aggregate data consumption in connection with Section IV of this Policy. However, in our effort to promote good citizenship within the Internet community, if we become aware of inappropriate use of the Service we will respond, at our discretion, in accordance with our policies and procedures, in each case in a manner we determine in our sole judgment and in accordance with applicable law. We have no obligation to monitor the Service and/or the network. We 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 our customers. We prefer to inform customers of inappropriate activities and give them a reasonable period of time in which to take corrective action. We also prefer to have customers directly resolve any disputes or disagreements they may have with others, whether customers or not, without our intervention. However, if the Service is used in a way that we, in our sole discretion, believe violates this Policy, we may take any responsive actions we deem appropriate under the circumstances with or without notice. These actions include, but are not limited to, temporary or permanent removal of content, filtering of Internet transmissions, and the immediate suspension or termination of all or any portion of the Service. Neither the Company nor our affiliates, suppliers, or agents will have any liability for any of these responsive actions. These actions are not our exclusive remedies and we may take any other legal or technical actions we deem appropriate with or without notice.

We reserve 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 and data on our servers and network. During an investigation, we may suspend the account or accounts involved and/or remove or block material that potentially violates this Policy. You expressly authorize and consent to the Company cooperating with (i) law enforcement authorities in the investigation of suspected legal violations and (ii) 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, we are authorized to

delete any files, programs, data, email and other messages associated with your account (and any secondary accounts).