Acceptable Use Policy

Please direct any questions or comments regarding this Acceptable Use Policy ("**AUP**") and complaints of violations of this AUP by subscribers to **internetabuse@fidomobile.ca.** Except where otherwise indicated, "**you**" and "**your**" means you and every person who uses the Services through your account.

Introduction

When using our services, the Equipment, our facilities or networks and any products, content, applications or services in conjunction with the Services or Equipment, you must comply with all applicable laws, and our policies, rules and limits including this AUP. This AUP supplements and is incorporated into the Fido Terms of Service (the "**Terms**"), which accompanies this AUP. It is also available at **fido.ca/terms**. Unless otherwise defined in this AUP, defined terms have the meanings given to them in the Terms.

IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS AND THIS AUP, AS AMENDED FROM TIME TO TIME, YOU SHOULD IMMEDIATELY STOP USING THE SERVICES AND NOTIFY FIDO THAT YOU ARE TERMINATING THE SERVICES.

Prohibited Activities

Without limitation, you may not use (or allow anyone else to use) our Services to:

1. use, possess, post, upload, transmit, disseminate or otherwise make available content that is unlawful or violates the copyright or other intellectual property rights of others (as described in more detail below);
2. participate in any illegal soliciting or gaming schemes;
3. attempt to use the Services in such a manner so as to avoid incurring charges for usage;
4. participate in any fraudulent activities, including impersonating any person or entity or forging anyone else's digital or manual signature. You assume all risks regarding the determination of whether material is in the public domain;
5. access the Internet via the Services using Internet Protocol (IP) addresses other than the IP address(es) assigned to you by us;
6. invade another person's privacy, collect or store personal data about other users, or stalk or harass another person or entity;
7. access any computer, software, data or any confidential, copyright protected or patent-protected material of any other person, without the knowledge and consent of that person, or use any tools designed to facilitate access, such as "**packet sniffers**";
8. upload, post, publish, deface, modify, transmit, reproduce, distribute in any way or otherwise make available information, software or other material protected by copyright or other proprietary or contractual right (such as a non-disclosure agreement) or related derivative works, without obtaining permission of the copyright owner or right holder;
9. use, reproduce, distribute, sell, resell or otherwise exploit the Services or content we provide or which you obtain through the Services for any commercial purposes;
10. copy, distribute, sub-license or otherwise make available any software or content we provide or make available to you or which you obtain through the Services, except as authorized by us;
11. alter, reproduce, or tamper with the Services or any function, component or identifier of your Equipment, such as the International Mobile Equipment Identity (IMEI) that is not meant to be altered, reproduced or tampered with;
12. restrict, inhibit or interfere with the ability of any person to access, use or enjoy the Internet, the Services or any Equipment used to connect to the Services, or create an unusually large burden on our networks or third party networks for which we have roaming or network sharing agreements, including, without limitation, posting, uploading, transmitting or otherwise making available information or software containing a virus, lock, key, bomb, worm, Trojan horse or other harmful, limiting, destructive or debilitating feature, distributing mass or unsolicited e-mail ("**spam**") or other messages, or otherwise generating levels of traffic sufficient to impede others' ability to send or retrieve information, or to use the Services in an abusive manner in connection with any unlimited packages, options or promotions;
13. disrupt any backbone network nodes or network service, or otherwise restrict, inhibit, disrupt or impede our ability to monitor or deliver the Services, any transmissions or data;
14. interfere with computer networking or telecommunications service to or from any Internet user, host, provider or network, including, without limitation, denying service attacks, overloading a service, improperly seizing or abusing

operator privileges ("**hacking**"), or attempting to "**crash**" a host;

15. use the Services for anything other than your own personal purposes (such as reselling the Services, providing Internet access or any other feature of the Services to any third party) or share or transfer your Services without our express consent;
16. operate a server in connection with the Services, including, without limitation, mail, news, file, gopher, telnet, chat, Web, or host configuration servers, multimedia streamers or multi-user interactive forums;
17. impersonate any person or entity, including, without limitation, a Fido official, forum leader, guide or host, or falsely state or otherwise misrepresent your affiliation with a person or entity;
18. forge headers or otherwise manipulate identifiers in order to disguise the origin of any content transmitted through the Services; or
19. port scan a person's computer or wireless device without that person's consent, or use any tools designed to facilitate these scans.

Unlawful or Inappropriate Content

Any Fido Party reserves the right to move, remove or refuse to post any content, in whole or in part, that it, in its sole discretion, decide are unacceptable, undesirable or in violation of the Terms or this AUP. This includes, without limitation:

1. obscene, profane, pornographic content;
2. defamatory, fraudulent or deceptive statements;
3. threatening, intimidating, abusive or harassing statements;
4. content that violates the privacy rights or intellectual property rights of others;
5. content that unlawfully promotes or incites hatred;
6. content that is otherwise offensive or objectionable; or
7. any transmissions constituting or encouraging conduct that would constitute a criminal offence, give rise to civil liability or otherwise violate any municipal, provincial, federal or international law, order or regulation.

For purposes of this AUP, "**content**" refers to all forms of communications including, without limitation, text, graphics (including photographs, illustrations, images, drawings, logos), executable programs, audiovisual recordings, and audio recordings.

Security

As set out above, you are responsible for any misuse of the Services, by you or by any other person with access to the Services through your Equipment or your account. Therefore, you must take steps to ensure that others do not gain unauthorized access to the Services through any means, including, without limitation, wireless networking and wired networking. The Services may not be used to breach the security of another user or to attempt to gain access to any other person's equipment, software or data, without the knowledge and consent of such person. Additionally, the Services may not be used in any attempt to circumvent the user authentication or security of any host, network, or account, including, without limitation, 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 networks. Use or distribution of tools designed for compromising security, such as password guessing programs, cracking tools, packet sniffers or network probing tools, is prohibited. You may not disrupt the Services. The Services also may not be used to interfere with computer networking or telecommunications services to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abuse of operator privileges and attempts to "**crash**" a host. The transmission or dissemination of any information or software that contains a virus or other harmful feature is also prohibited. You are solely responsible for the security of any device you choose to connect to the Services, including any data stored on that device. In particular, Fido recommends against enabling file or printer sharing of any sort. Fido recommends that any files or services you do choose to make available for remote access be protected with a strong password or as otherwise appropriate. You agree to treat as confidential all access codes, personal identification numbers and/or other passwords that we may provide to you for use with the Services.

Unsolicited Communications

As set out above, the Services may not be used to send unsolicited, bulk or commercial messages or for any other unsolicited communications. This includes, without limitation, using automatic dialing and announcing devices to or otherwise make unsolicited voice or facsimile calls and bulk mailing of commercial advertising, informational announcements, charity requests, petitions for signatures and political or religious messages. Such communications may only be directed to those who have explicitly requested it. The Services may not be used to send messages to any individual who has indicated that he/she does not wish to receive messages from you. The Services may not be used to collect responses from unsolicited e-mail messages sent from accounts on other Internet hosts or e-mail services that violate this AUP or the acceptable use policy of any other Internet service provider. Moreover, unsolicited e-mail messages may not direct

the recipient to any web site or other resource that uses the Services. Forging, altering or removing e-mail headers is prohibited. You may not reference any Fido network (for example, by including "**Organization: Fido**" in the header or by listing an IP address that belongs to a Fido network) in any unsolicited e-mail even if that e-mail is not sent through a Fido network. "**Mail bombing**" is prohibited. That is, you may not send numerous copies of the same or substantially similar messages, nor may you send very large messages or files to a recipient with the intent to disrupt a server or account. The propagation of chain letters is similarly prohibited, whether or not the recipient wishes to receive such mailings. Fido is not responsible for the forwarding of e-mail sent to any account that has been suspended or terminated. Such e-mail will be returned to sender, ignored, deleted, or stored temporarily, at Fido's sole discretion.

User-Generated Content Services

"**User-Generated Content Services**" or "**UGC Services**" refers to any services that allow an end user to post, upload or generate content online to be shared with a limited or unlimited number of recipients and may include, without limitation: newsgroups, online forums, message boards, chat programs, wiki's, photo sharing services, customer review sites, video sharing services, blogs and web hosting.

Any User-Generated Content Services accessed through the Services must be used in accordance with the following:

1. you must comply with the UGC Service's written charter, policies or FAQs;
2. you may only post advertisements, solicitations, or other commercial messages in the UGC Service if that service's charter, policies or FAQs explicitly permit them;
3. you are responsible for determining the policies of the UGC Service before using it;
4. you must adhere to daily volume, file size and format restrictions of any UGC Service;
5. unless otherwise specified in the UGC Service's charter, policies or FAQs, you must not forge, alter or remove any information from the UGC Service;
6. the Fido Parties have no obligation to monitor the content of any UGC Service and the Fido Parties are not liable for any claims, losses, actions, proceedings, suits, liabilities, damages, settlements, penalties, fines, costs and expenses arising out of or relating to the content of any such service;
7. you must not use the UGC Service to perform "**flooding**", which refers to deliberately repeating actions in quick succession in order to fill the screens of other Internet users with text or other content;
8. any computer or other device connected through the Services may not maintain more than two simultaneous chat connections including, without limitation, the use of automated programs, such as "**bots**" or "**clones**". Automated programs may not be used when the account holder is not physically present at the device;
9. you must not use the Services to send messages that disrupt another user's equipment, software, hardware or user display; and
10. you must not forge, alter or obscure your identity (other than using a nickname) while participating in the UGC Service.

Usage, Data Storage and Other Limitations

You must comply with the then current usage, data storage and other limitations on your applicable Services. You must also ensure that your activity does not improperly restrict, inhibit, or degrade any other subscriber's use of the Services, nor represent (in the sole judgment of Fido) an unusually large burden on our networks or third party networks for which we have roaming or network sharing agreements. In addition, you must ensure that your activity does not improperly restrict, inhibit, disrupt, degrade or impede Fido's ability to deliver the Services, and monitor and investigate the Services, backbone, network nodes, and/or other network services or components. You may not resell, share, or otherwise distribute the Services or any portion thereof to any third party without the written consent of Fido. For example, you cannot provide Internet access to others through a dial up connection, host shell accounts over the Internet, provide e-mail or news service, or send a news feed. The Services are consumer products designed for personal purposes. For example, the Services do not provide the type of security, upstream performance and total downstream throughput capability typically associated with commercial use. You may not run a server in connection with the Services. You may not provide network services to others via the Services. In addition, you are prohibited from running servers for mail, http, ftp, irc, and dhcp, and multiuser interactive forums.

Your use of the Services may be subject to a usage limit, as set out in your Agreement. If you exceed that limit, you may be subject to additional usage charges.

Network Management

We reserve the right to manage our networks (or third party networks for which we have roaming or network sharing agreements) in order to optimize their efficiency for the benefit of our subscribers, including, without limitation, by way of the following: rate limiting (speed), rejection or removal of spam or otherwise unsolicited bulk e-mail, anti-virus mechanisms, and protocol filtering. We may take any other

action we deem appropriate in order to help ensure the integrity of the network experience for all subscribers. For details on our network management practices check out our **network policy**.

Violation of this Acceptable Use Policy

As set out in the Terms, we have the right, but not the obligation, to monitor or investigate any content that is transmitted using the Services (other than voice Services) or the Equipment; and to access or preserve content or information in accordance with the Terms. We prefer to advise subscribers of inappropriate behavior and any necessary corrective action. However, if the Services are used in a way that we, in our sole discretion, believe violates this AUP, any of the Fido Parties may take any responsive actions they deem appropriate. Such actions may include, without limitation, temporary or permanent removal of content, cancellation of newsgroup posts, filtering of Internet transmissions, and/or the immediate suspension or termination of all or any portion of the Services or your account. The Fido Parties will have no liability for any such responsive actions. The above described actions are not exclusive remedies and the Fido Parties may take any other legal or technical action deemed appropriate. Upon termination of an account, any of the Fido Parties are authorized to delete any files, programs, data and e-mail messages associated with such account. The failure to enforce this AUP, for whatever reason, shall not be construed as a waiver of any right to do so at any time. If any portion of this AUP 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. This AUP shall be exclusively governed by, and construed in accordance with the governing law provision set out in the Terms.

Complaints

Please direct any complaints of violations of this AUP to **internetabuse@fidomobile.ca** or contact us at 1-888-481-3436. Questions or complaints, concerning third party content should be addressed to the applicable content provider.

FIDO NETWORK MANAGEMENT POLICY

Wireline

Fido relies on network investments as the primary tool to manage Internet traffic and address potential congestion. We monitor the utilization of the wireline Internet network to maintain the service experience and plan for additional capacity to ensure that our customers continue to receive the broadband speeds they have purchased.

Fido has mechanisms in place to protect our wireline Internet network from malicious traffic and security threats, such as Denial of Service (DOS) attacks, malware, spam, and fraudulent activity (e.g., modem cloning). We take standard, necessary and reasonable steps to prevent service outages and to ensure that bandwidth usage is optimized efficiently amongst our customers who share the same service node.

In times of emergencies and extreme circumstances, or cases of disproportionate use of the network, Fido may also apply the following technical Internet traffic management practice (ITMP) to our wireline Internet service:

1. What is the ITMP and when will it occur:

Fido's traffic management policy for our retail wireline Internet service comes into effect in the event of significant network congestion as the result of:

a) an emergency or extreme circumstance; or

b) a customer's activity that restricts, inhibits or degrades other customers' use of the service or Fido's ability to deliver the service.

During such instances, Fido may deploy a traffic management measure to a customer's upload traffic (i.e. from the customer to the Internet) on wireline Internet service plans with a maximum upload speed of 10 Mbps or higher.

Should a customer engage in a volume of upload activity over a sustained period of time such that this usage negatively impacts, or is likely to negatively impact, the Internet experience for other customers, that customer's maximum upload speed may be temporarily reduced.

2. Why the ITMP is applied:

Fido deploys this traffic management measure so that all Fido Internet customers receive fair access to the Internet. During periods of significant network congestion resulting from emergency or extreme circumstances, or a customer's disproportionate use of the network, this helps to ensure that all of our customers can enjoy a consistent and reliable online experience and preserves the integrity of our network.

This objective is especially important in times of public emergency that result in greater demands on our network. During such periods, keeping our customers connected to their families, friends and co-workers – and to critical information and services – is essential.

3. What type of Internet traffic (e.g. application, class of application, protocol) is subject to the ITMP:

No specific application or protocol is specifically targeted through this traffic management policy.

Only data upload activity described under #1 above may be subject to traffic management. Download traffic is not managed.

Fido's traffic management policy is designed to reduce the impact of extreme, data-intensive activity by individuals during a congested period in order to leave resources open for more customers engaging in real-time interactive activities.

4. How the ITMP will affect a user's Internet experience, including the specific impact on speeds:

If a customer's maximum upload speed is temporarily reduced as a result of this ITMP, it may take longer to upload larger volumes of data.

Under the ITMP, maximum upload speeds will be maintained at levels that will continue to support real-time interactive activities, such as online banking, web-browsing, social networking, audio/video conferencing, online gaming and VoIP services.

For the vast majority of our customers, their Internet experience is unaffected by our traffic management policy.

Fido Mobile

Fido relies on network and spectrum investments as the primary tool to manage mobile Internet traffic and address potential congestion. We have mechanisms in place to protect the Fido wireless network and our customers from malicious traffic and other security threats, as well as standard network management processes to enable the normal operation of our mobile network.

Fido may also enhance performance of its mobile wireless network by optimizing video streaming. Optimizing video streams may result in faster load times and fewer or no playback interruptions or stalls during common mobile usage. Due to the small screen size of a smartphone or tablet, the impact on image quality should be minimal or unnoticeable. Video optimization can also lower mobile customers' data usage and create less network congestion. Optimization may occur with all detected video streamed over the Fido network in Canada (including Extended Coverage), as well as foreign networks. Optimization does not apply to streaming over WiFi, video messages or conferencing, nor to videos saved to your device.

Rogers First Priority Service provides priority access to first responders, public safety officials, and critical infrastructure personnel. In the rare event that demand for network resources exceeds expected peak capacity, such as during natural disasters or threats to public safety, data connections from these users are prioritized by the mobile network.

As a result, during these rare events, Fido users connecting to sites in the same area may experience slightly slower speeds and delayed response times when using data services, such as browsing and uploading or watching videos (all applications treated equally). In extremely rare cases, data connections could need to be re-initiated. 9-1-1 service is never impacted.

Specific plans may have Internet traffic management practices applied as outlined in their data management policies (as listed below).