System Use Policies / Unacceptable Conduct

The following activities are listed as examples of conduct that may lead to limitation, suspension or termination of your service. We may, but are not required to, monitor your compliance or the compliance of other subscribers with its terms, conditions or policies. You acknowledge that we shall have the right, but not the obligation, to pre-screen, refuse, move or remove any content available on the Service, including but not limited to content that violates the law or this AUP.

1. Transmission, distribution or storage 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, defamatory, constitutes an illegal threat, or violates export control laws.

   In accordance with the Digital Millennium Copyright Act (DMCA), an agent has been designated to receive notification of a claimed copyright infringement for Peoples . Any claims of copyright infringement should be directed to:

   WHO and what email address?

2. Customer has no ownership of static IP numbers that may have been assigned to the customer by Peoples. Peoples reserves the right at any time to remove these static IP assignments with advance notice to the customer from Peoples. If deemed necessary, Peoples also reserves the right to reassign static IP allocation at its sole discretion.
   a. The services you purchase from Peoples are not transferable. The reselling of all Internet Access Services is strictly prohibited unless expressed permission is received in writing from Peoples. Internet Access Services are not to be shared with a second entity, extended, redistributed or retransmitted via wired or wireless networks outside the primary location without expressed permission in writing from Peoples.
   b. Peoples knows that a customer's use of available bandwidth may "peak" for short periods of time when viewing streaming video, uploading/downloading a large file or sending large e-mails, and Peoples will attempt to avoid limiting bandwidth availability in those instances. However, when a customer's peak use impacts the performance of other customers' services, Peoples reserves the right to take steps to maintain the integrity and performance characteristics of its network, which may include steps to limit your bandwidth.
   c. Peoples will use a network utilization, monitoring and reporting system to identify and confirm excessive use, Peoples' network management practices are designed to function neutrally, permitting (1) access to lawful content of the subscriber's choice, (2) running applications and accessing services of the subscriber's choice (subject to the needs of law enforcement), and (3) connection to the subscriber's choice of legal devices that do not harm the network.
   d. Peoples will make a good faith and reasonable effort to contact a customer Peoples believes is making excessive use of its Internet Services, currently defined as exceeding 100 G-bytes per month, prior to limiting bandwidth, and to discuss ways the customer may avoid such limitation. However, customers whom Peoples determines to be making

excessive use of Peoples Internet Services may have service limited, metered, suspended or, if necessary, terminated.

3. Sending uninvited communications, data or information, including, without limitation, "flaming," or Unsolicited Bulk Email ("UBE", "spam") through Peoples servers is prohibited. Likewise, the sending of UBE from another service provider advertising a web site, email address or utilizing any resource hosted on Peoples servers, is prohibited. Peoples accounts or services may not be used to solicit customers from, or collect replies to, messages sent from another Internet Service Provider where those messages violate this AUP or that of the other provider.

4. Running Unconfirmed Mailing Lists. Subscribing email addresses to any mailing list without the express and verifiable permission of the email address owner is prohibited. All mailing lists run by Peoples customers must be Closed-loop ("Confirmed Opt-in"). The subscription confirmation message received from each address owner must be kept on file for the duration of the existence of the mailing list. Purchasing lists of email addresses from 3rd parties for mailing to/from any Peoples hosted domain, or referencing any Peoples account, is prohibited.

5. Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, which includes, but is not limited to, the facilitation of the means to send Unsolicited Bulk Email, initiation of pinging, flooding, mail-bombing, or denial of service attacks.

6. Operating an account on behalf of, or in connection with, or reselling any service to, persons or firms listed in the Spamhaus Register of Known Spam Operations (ROKSO) database at www.spamhaus.org.

7. Unauthorized attempts by a user to gain access to any account or computer resource not belonging to that user (e.g., "cracking") are prohibited.

8. Intercepting, interfering with or redirecting email or other transmissions sent by or to others is prohibited.

9. Introducing viruses, worms, harmful code or Trojan horses is prohibited.

10. Defamatory conduct is prohibited.

11. Obtaining or attempting to obtain any of the Internet Services by any means or device with intent to avoid payment is prohibited.

12. Unauthorized access, alteration, destruction, or any attempt thereof, of any information or the accounts of any other person or entity by any means or device is prohibited.

13. Engaging in any activities designed to harass, or that will cause a denial-of-service (e.g., synchronized number sequence attacks) to any other user whether on the Peoples network or on another provider's network is prohibited.

14. Using Peoples Internet Services to interfere with the use of the Peoples network by other customers or authorized users is prohibited.

15. Content posted to Peoples Personal Web Pages will be removed if that content violates copyrights, libels others, or contains code which could harm systems which visit the site.

16. Sexually explicit and patently offensive content; materials that otherwise violate federal, state or local law; and materials and content that threaten the security or utility of the Peoples network, are strictly forbidden in any Peoples Web service to which you subscribe -- personal or commercial.

17. You may not use Peoples Internet Services to gain, or attempt to gain unlawful access to other computer or other computer systems.

18. Peoples reserves the right to remove from public view any material or content brought to its attention which violates this AUP.

19. Forgery or impersonation. Adding, removing or modifying identifying network header information in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous remailers or nicknames does not constitute impersonation. Using deliberately misleading headers ("munging" headers) in news postings in order to avoid spam email address collectors is allowed.

20. Harm to minors. Using the Internet Services to harm, or attempt to harm, minors in any way is prohibited.

21. Threats. Using the Internet Services to transmit any material (by email, uploading, posting, or otherwise) that threatens or encourages bodily harm or destruction of property is prohibited.

22. Harassment. Using the Internet Services to transmit any material (by email, uploading, posting, or otherwise) that harasses another is prohibited.

23. Fraudulent activity. Using the Internet Services to make fraudulent offers to sell or buy products, items, or services or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters" is prohibited.

24. Collection of personal data. Using the Internet Services to collect, or attempt to collect, personal information about third parties without their knowledge or consent is prohibited.

25. Using a personal account for high volume or commercial use is prohibited.