

Education Networks of America APU

All Users of ENA's Services are bound by and must comply with this Acceptable Use Policy ("AUP"). Account Holders are additionally responsible for ensuring that Users who access the Services through the Account Holder's account are aware of and comply with this AUP.

Definitions

"Account Holder" means an entity or individual who has established an account for ENA Services.

"AUP" means this Acceptable Use Policy, as it may be amended from time to time as described below.

"ENA" means Education Networks of America, Inc. together with any of its subsidiaries, parent companies, trade names or affiliates.

"Services" means the internet access, e-mail, hosting, collocation, or any other services provided to you by ENA through which you have access to or utilize any network operated by or on behalf of ENA..

"Users" or "You" or similar terms means (i) the Account Holder, and (ii) each individual who gains access to the Services through the Account Holder's account.

General

This AUP is intended to assist in protecting ENA, our Users, and the Internet community as a whole from improper and/or illegal activity over the Internet. Users are generally expected to behave in a reasonable fashion and to adhere to commonly accepted practices of the Internet community. For the most part, simply exercising good judgment and common sense while using the Services should enable Users to comply with this AUP. The items discussed in this AUP are intended merely to serve as guidelines regarding appropriate and inappropriate conduct, but these items are not intended to be exhaustive nor should they be interpreted as such.

INDIRECT OR ATTEMPTED VIOLATIONS OF THIS AUP BY YOU, AND ACTUAL AND ATTEMPTED VIOLATIONS OF THIS AUP BY A THIRD PARTY ON YOUR BEHALF, SHALL BE CONSIDERED VIOLATIONS OF THIS AUP BY YOU.

ENA will not, as an ordinary practice, proactively monitor the activities of its Users to ensure that its Users comply with this AUP and/or the law. If ENA is alerted to a possible violation of this AUP, ENA will take whatever measures it deems necessary to stop or prevent those violations, including the actions described in this AUP.

Modifications to AUP

ENA may revise this AUP at any time by posting the revised AUP to a clearly-identified URL accessible from within ENA's website, which has its home page at www.ena.com. Your continued use of the Services after any revisions have been posted shall constitute your binding acceptance of the revised AUP. To receive notification of AUP updates, subscribe your e-mail address to the AUP List at <http://lists.ena.com/mailman/listinfo/aup-updates>.

Spam / Unsolicited Commercial E-mail

Use of the Services in connection with any of the following activities is strictly prohibited:

sending unsolicited commercial or unsolicited bulk e-mail messages or other electronic communications (including ICQ, IRC, instant messenger services, Windows Messenger Service, etc.);

collecting responses from mass unsolicited e-mail messages or other electronic communications (including ICQ, IRC, instant messenger services, Windows Messenger Service, etc.);

“mail bombing”, i.e. sending (i) excessively large volumes of e-mail messages, or (ii) e-mail messages with excessively large file attachments to a recipient, where a purpose or likely result of the activity is to impede, interfere with or otherwise negatively affect the ability of any third party to use the Internet or to conduct business over the Internet or to negatively affect the operation of any web site, host or network;

SMTP relays or similar relays to or from a third party’s electronic mail server, unless previous authorization has been obtained from the owner of the remote system;

hosting websites or offering services that support spamming or mail bombing or that cause or may, in ENA’s opinion, cause any IP address or range of IP addresses assigned to ENA to be listed in any spam database.

Unauthorized Access to Networks / Denial-of-Service Attacks

A User may not attempt to gain unauthorized access to, or attempt to interfere with or compromise the normal functioning, operation, or security of any network, system, computing facility, equipment, data, or information. A User may not use the Services to engage in any activities that may interfere with the ability of others to access or use the Services or the Internet. A User may not use the Services to monitor any data, information, or communications on any network or system without authorization. A User may not attempt to gain unauthorized access to the user accounts or passwords of any third party. For further clarification, any activity that might be a precursor to any such activity (i.e. port scans, stealth scans, or other information gathering activities) is also prohibited.

Passwords and Security

You are entirely responsible for maintaining the confidentiality of your password and account information, as well as the security of your network. You must adopt adequate security measures to prevent or minimize unauthorized use of your network or account. It is your responsibility to ensure that your network is configured in a secure manner, and you may not permit your network, through action or inaction, to be configured in such a way that a third party may use your network in an illegal or inappropriate manner. You agree immediately to notify us of any unauthorized use of your account or any other breach of security known to you. Should any of your systems be violated, you are responsible for reporting the violation and then fixing the exploited system. You are responsible for any misuse of your account, even if a friend, family member, guest, employee or other person committed the inappropriate activity.

Fraudulent Headers / Spoofing / Munging

Users may not initiate any e-mail message or transmit any other electronic communication that contains fraudulent, fake, hidden, or incomplete header information or other identifying information such that any recipient of the transmission might be deceived as to the source of the transmission. Users are

prohibited from intentionally or negligently injecting false data into the Internet, for instance in the form of incorrect or fraudulent routing information or incorrect DNS information. Notwithstanding the foregoing, munging of e-mail addresses in headers (i.e. the practice of altering an e-mail address such that the address will be unusable or undetectable by programs that build e-mail lists for spamming purpose) is permitted, provided that it is done in such a way that a person reading the document (as opposed to a program scanning it) can easily discern that it is a munged e-mail address, and can easily and unmistakably deduce the true e-mail address.

USENET / Bulletin Board Postings

All postings to USENET groups, bulletin boards, e-mail lists, or similar online public services must comply with that group's charter and policies. Commercial posts are prohibited unless expressly permitted by the charter or policies of the group.

Excessive Use

If we have specified bandwidth or other usage limitations for your user account, use of the Services shall not be in excess of those limitations. Furthermore, you may not use resource-intensive programs that negatively impact other ENA customers or the performance of ENA systems or networks. ENA reserves the right to terminate or limit such activities in its sole discretion.

Intellectual Property Rights

Users may not use the Services in any manner or in connection with or in support of any activity prohibited by applicable law, including, without limitation, treaties, tariffs, laws governing intellectual property rights, and export control laws.

Obscene or Harmful Materials

Users may not use the Services to advertise, transmit, store, post, display, or otherwise make available any material that ENA determines, in its sole discretion, is obscene, defamatory, harassing, abusive, or threatening. Specifically, in those instances involving child pornography, ENA complies with all applicable federal or state laws, including providing notice to the NationalCenter for Missing and Exploited Children or other designated agencies.

Compromised Servers

Where ENA is providing collocation services, Users shall take all commercially reasonable precautions to ensure that their servers do not become compromised. A compromised server is one that has been accessed or manipulated by any third party not authorized by the User or ENA. As a compromised server is potentially disruptive to the ENA network and to other ENA customers, ENA cannot allow a compromised server to remain online for extended periods of time. Therefore, once ENA has determined that a server has been compromised and ENA has notified the affected User of the compromised server, the User will have 24 hours from that time to agree to one of the options offered by the ENA's support team to rectify the problem and secure the server. If there has been no response at the end of the 24 hour period or if the User responds but does not agree to one of the options offered by the ENA support team, the compromised server will be taken offline and all access to and use of such compromised server will be suspended. The User will then have 5 days after the date of suspension of the compromised server to contact ENA to resolve the issue. If the issue is not resolved to the

satisfaction of ENA after 5 days, the compromised server will be removed permanently from our network. Notwithstanding the foregoing, where a compromised server is actively attacking other networks or other disrupting other ENA customers, ENA will act to protect the integrity of its network and will suspend or permanently terminate access to and use of such compromised server immediately without prior notice to customer.

Other Prohibited Activities

Use of the Services in connection with any of the following activities is strictly prohibited:

Violating any rules, regulations or policies applicable to any network, server, web site, computer database, or internet service provider that you access through the Services.

Any fraudulent offers to buy or sell products, items or services or to advance any type of financial scam such as "pyramid schemes", "Ponzi schemes" and "chain letters".

Intentionally transmitting Internet viruses, worms, trojan horses, or similar malicious code.

Attempting to intercept, redirect, or otherwise interfere with communications intended for others.

Intentionally transmitting files containing a computer virus or corrupted data.

Running any program or taking any other action designed to defeat network inactivity time-outs.

Resale of ENA's services or products, unless expressly authorized in a separate written agreement with ENA.

Harassment, whether through language, frequency, or size of messages.

Using the Services to harm, or attempt to harm, minors in any way.

Furnishing false or incorrect data to ENA on written or online applications, contracts, or other materials or information provided to ENA, including fraudulent use of credit card numbers or other billing information.

Attempting to circumvent or alter the processes or procedures to measure time, bandwidth utilization, or other methods to document use of ENA's products and services.

Hosting an IRC server that is part of or connected to another IRC network or server.

Servicing, altering, modifying or tampering with any ENA equipment or service or permitting any other person to do the same, without ENA's explicit written authorization.

Collecting, or attempting to collect, personal information about third parties without their knowledge and consent.

Any activity that ENA, in its sole discretion, determines to be harmful to its customers, operations, reputation or goodwill.

Any illegal activity, whether or not specifically listed in this AUP.

Any other inappropriate activity or abuse of the Service (as determined by us in our sole discretion), whether or not specifically listed in this AUP.

Enforcement

If you engage in conduct while using the Services that is in violation of this AUP or is otherwise illegal or improper, we reserve the right to suspend and possibly terminate the Services or one or more Users' access to the Services. In most cases, we will attempt to notify you of any such activity and request that the you cease such activity; however, we reserve the right to suspend your Services or a User's access to the Service without notification. In addition, we may take any other appropriate action, legal or otherwise, against a User for violations of this AUP, which may include termination of the Services. We

do not make any promise, nor do we have any obligation, to monitor or police activity occurring via the Services and will have no liability to any party, including you, for any violation of AUP.

In addition to suspending or terminating Services or User accounts, we may also take any other action that we deem appropriate in response to a violation of this AUP, and nothing in this AUP shall be deemed as a waiver of any other remedy that we may have in law or in equity.

Reporting of Violations

If you become aware of any violation of this AUP by any person, including Users that have accessed the Services through your account, please notify us immediately. You agree to promptly investigate all such complaints and take all necessary actions to remedy any actual violations of this AUP. We may identify to the complainant that you are investigating the complaint and may provide the complainant with the necessary information to contact you directly to resolve the complaint. We reserve the right to install and use, or to have you install and use, any appropriate devices to prevent violations of this AUP, including devices designed to filter or terminate access to the Services provided by us.

Complaints

Complaints about violations of this AUP should be directed to abuse@ena.com. Complaints should contain as much supporting information as possible, including (if available):

All available header or IP information.

The date and time of the alleged violation including the time zone or offset from GMT.

Evidence of the alleged violation.

Valid contact information for the complaining party so that we may request clarification or further details.