

Chatham University Electronic Honor Code Responsible Use Policy Regarding the Use and Abuse of Computers and Network Systems

The Responsible Use Policy **applies to all faculty, students and staff**. It expands on the principles of behavior that were incorporated into the Honor Code for guiding the use of computers and networks. The basic premise is that legitimate use of a computer or network does not extend to whatever an individual is capable of doing with it.

Violations of the Responsible Use Policy are handled by the Chatham Student Government (CSG) according to the procedures defined in the Honor Code (HC). Alleged violations of this policy can be reported directly to the Director of Information Technology. If the person responsible is not affiliated with the University, or cannot be identified, the incident should be reported to helpdesk@chatham.edu. In addition, some instances may violate federal law. See the Federal Computer Security Violations (<http://www.cybercrime.gov/cc.html>) for more information.

The following are examples of policy violations and not intended to be a comprehensive list.

- **Accessing, or attempting to access, another individual's data or information without proper authorization** (e.g. using another's Network ID and password to look at their personal information).
- **Obtaining, possessing, using, or attempting to use someone else's password regardless of how the password was obtained** (e.g. password sharing).
- **Tapping phone or network transmissions, including wireless transmissions** (e.g. running network sniffers without authorization).
- **Making more copies of licensed software than the license allows** (i.e. software piracy).
- **Sending a crippling number of files across the network** (e.g. e-mail "bombing" or "spamming").
- **Releasing a virus, worm or other program that damages or otherwise harms a system or network.**
- **Preventing others from accessing services** (e.g. allowing a file-sharing application, such as KaZaA, Morpheus, BitTorrent or any of its variations (BitComet), LimeWire, Aries etc. to generate a volume of traffic that cripples/inhibits/retards other users' network access).
- **Unauthorized use of college resources.**
- **Sending forged messages under someone else's network name** (e.g. sending hoax messages, even if intended to be a joke).
- **Using college resources for unauthorized purposes** (e.g. using personal computers connected to the campus network to set up web servers for illegal, commercial or profit-making purposes).

- **Unauthorized access to data or files even if they are not securely protected** (e.g. breaking into a system by taking advantage of security holes, or defacing someone else's web page).

Responsible Use of Electronic Communications

The University cherishes the diversity of values and perspectives endemic in an academic institution and so is respectful of freedom of expression. The University does not condone censorship, nor does it endorse the inspection of electronic files other than on an exceptional basis. As a result, the University cannot protect individuals against the existence or receipt of material that may be offensive to them. The University encourages individuals to use electronic communications in a responsible manner. Finally, the policy includes information about behavior that would constitute a violation and contains a set of procedures for reporting incidents.

Policy violations fall into four categories that involve the use of electronic communications to:

- **harass, threaten, or otherwise cause harm to a specific individual(s)**; for example, sending an individual repeated and unwanted (harassing) e-mail or using e-mail to threaten or stalk someone.
Alleged violations of this type can be reported directly to the Director of Residence Life or to Campus Police if the situation is potentially serious and requires immediate attention. If the person responsible is not affiliated with the University or if it is not possible to identify the individual, the incident can still be reported to the police. These offices can assist by referring to appropriate sources outside the University.
Save electronic copies of all correspondence for evidence.
- **impede, interfere with, impair, or otherwise cause harm to the activities of others**; for example, propagating electronic chain mail, or sending forged or falsified e-mail.
Alleged violations of this type can be reported to helpdesk@chatham.edu. If the person responsible is not affiliated with the University, the incident should be reported to the site that provides the individual with Internet access. If it is not possible to identify the origin, contact the Chatham College Help Desk for assistance.
Save electronic copies of anything that can be used as evidence.
- **download or post to University computers, or transport across University networks, material that is illegal, proprietary, in violation of University contractual agreements, or otherwise is damaging to the institution**; for example, launching a computer virus, distributing child pornography, distributing copyrighted musical recordings via a file-sharing application, or posting a University site-licensed program to a public bulletin board. Alleged violations of this type can be reported directly to helpdesk@chatham.edu
- **harass or threaten classes of individuals.**
Alleged violations of this type can be reported directly to the Campus Police. If the person responsible is not affiliated with the University, the incident should be reported to the site that provides the individual with Internet access. If it is not possible to identify the origin, contact the Chatham University Help Desk for assistance. **Save electronic copies of anything that can be used as evidence.**

What are some violations of Chatham University policy?

The section on university-wide Policies and Codes describes what activities constitute responsible use as well as violations. Following is more detail about some violations that Information Technology frequently receive questions about.

- **Sharing Network names and passwords (unauthorized use)**

Your network ID and password are provided only for your use. Network IDs provide access to a wide range of services that are restricted for use by you personally (such as grades, address information, email, benefits) or are restricted for use by the Chatham community (such as e-mail, library services). If you share your network ID with spouses, family members, friends or roommates, then you are giving them access to services they are not authorized to use. They will also have access to all of your personal information. They may even embarrass you by sending email in your name or by modifying your web page.

DO NOT SHARE YOUR PASSWORD WITH ANYONE. If you suspect that someone may have discovered your password, change it immediately.

DO NOT USE ANYONE ELSE'S PASSWORD. Using someone else's password to access services or data is also a violation of policy, regardless of how the password was obtained.

- **Chain e-mail and virus hoaxes**

The most important thing to remember if you get chain e-mail is: **do not help propagate it.** Chain e-mail usually contains phrases like "pass this on", "forward - do not delete", "don't break the chain", "this is safe, don't worry", "let's see how long this takes to get back to the start", "this has been around the world 20 times", "7 years of good luck!", "I don't wanna die", "your mom would want you to do this", etc. Often there is some story about how lucky a person has been since they forwarded the chain e-mail, or how unlucky they were because they didn't. Sometimes chain e-mail is disguised - it tells of a child who is dying and wants post cards, or it warns about e-mail viruses or internet shutdowns. Don't fall for it. It's all chain mail and it's designed to get you to forward it.

In recent years, chain mail **hoaxes** of various sorts have become widespread on the Internet. Some are virus warnings like "Good Times", "PenPal", and "Irina". Others are like the "Naughty Robot" that claims to have all your credit card numbers. They tell you to forward the "warning" to everyone you know. Most hoaxes start out as pranks, but often live on for years, getting passed around by new people who have just joined the Internet community. Don't believe every warning you get via e-mail. You should not pass these warnings on unless you verify the authenticity. You should contact the HelpDesk or helpdesk@chatham.edu or check out one of the many sites on the Internet that track hoaxes:

- o [Vmyths.com](http://www.vmyths.com/) (<http://www.vmyths.com/>)
- o [National Fraud Information Center](http://www.fraud.com/) (<http://www.fraud.com/>)

If you get chain e-mail from someone with a Chatham e-mail address, you can report it to the HelpDesk or helpdesk@Chatham.edu. You will need to include a copy of the chain e-mail in your report. In most cases, a first offense results in a warning. Subsequent offenses result in a referral to the CSG for disciplinary action. If you get chain e-mail from someone not affiliated with Chatham, you can reply to the sender

and let them know you are not happy about getting chain e-mail from them, or you can delete and ignore it. Most places have policies regarding the propagation of chain e-mail and will deal with it on their end.

- **Harassment**

Electronic communication that is repeated and unwanted may constitute harassment. In general, communication targeted at a specific individual with the intent to harass or threaten is a violation of Chatham policy. If you receive unwanted e-mail or another form of communication, you may want to consider notifying the sender that it is unwanted. Many times a person will not realize that their communication is unwanted unless you tell them. If the sender continues to communicate after being placed on notice, or if you feel uncomfortable confronting the sender, the incident should be reported to the Director of Residence Life. You should also contact the Chatham police if the situation is potentially serious and requires immediate attention. **Save electronic copies of anything that can be used as evidence.**

- **Forgery**

Altering electronic communications to hide your identity or impersonate another person is considered forgery. All e-mail, news posts, or any other form of communication using college systems should contain your name and/or network ID. Forgery includes using another person's identity or using an identity that's fake (like god@heaven or anon@nowhere). Forgeries intended as pranks or jokes are still considered violations.

- **Tapping phone or network transmissions**

Running a network "sniffer" program to examine or collect data from the network, including wireless networks, is considered tapping a network.

- **E-mail bombing**

Flooding someone with numerous or large e-mail messages in an attempt to disrupt them or their site is known as "e-mail bombing". Often this is done to retaliate because someone has done something annoying. But more often than not e-mail bombing will either cause problems for your local system or disrupt service for thousands of other innocent bystanders. If you are having a problem with someone, pursue an acceptable method to report the situation. If it's a Chatham person, then refer to University-wide Policies and Codes and determine what violation is occurring and report it as outlined for that type of violation.

- **Interfering with activities of others**

This can be any activity that disrupts a system and interferes with other people's ability to use that system. In some cases, consuming more than your "fair" share of resources can constitute interference. Some examples are:

- e-mail bombing that causes a disk to fill up, the network to bog down, or an e-mail application to crash;
- posting many messages to a single news group or mailing list making it difficult for subscribers to carry on their normal discussion;
- running a file-sharing application such as KaZaA, Morpheus, LimeWire, or BitTorrent that slows down the network by consuming excessive bandwidth.

- **Unauthorized access**

As stated in the Policy Regarding Abuse of Computers and Networks, legitimate use of a computer or network does not extend to whatever an individual is capable of doing. In some cases, operating systems have security holes or other loopholes that

people can use to gain access to the system or to data on that system. This is considered unauthorized access. If someone inadvertently turns on file sharing on their personal computer, you do not have the right to read or delete their files unless you have been given explicit permission from the owner. This is much like accidentally leaving your house door unlocked. You wouldn't expect a burglar to use that as an excuse for robbing you.

- **Commercial use of University resources**

Using e-mail to solicit sales or conduct business, setting up a web page to advertise or sell a service, or posting an advertisement to a news group all constitute commercial use. Even if you use your own personal computer, but you use the University's network (either from a dorm room, office or via dial-up access from home), you are in violation of the policy.

- **Adult pornography**

Accessing or publishing pornographic or demeaning materials on University owned electronic equipment (including but not limited to: computer desktops, servers, laptops and tablet PCs) is prohibited. Some material available on the Internet is considered objectionable to others. Chatham University is not responsible for materials accessed or published by users. The computer lab facilities are for the use of all, and those wishing to use the labs may not display, transfer or save magnetically or electronically, print or copy demeaning materials. This includes, but is not limited to, pornography, "how to" documents encouraging violence or illegal acts, and racist tracts or hate speech.

- **Illegal activities**

Listed under "What is illegal under local, state and federal laws?" are all items considered to be violations of University policy. This is not a comprehensive list, nor is it intended to be, but it contains the activities most frequently asked about.

What are NOT violations of Chatham University policy?

- **Unsolicited e-mail or junk e-mail**

The amount of unwanted or unsolicited e-mail (junk mail) has increased as more people take advantage of Internet communications. The same kinds of things come in the U.S. Postal mail on a regular basis - catalogs, advertisements, solicitations, and political propaganda are some examples. This form of speech is usually protected under the first amendment, even though some people may find some of the content objectionable. Chatham does use a monitoring tool to filter some junk e-mail. You will receive notifications in your email box when messages have been stopped by the spam filter.

Remember that junk mail is NOT illegal and it is NOT a violation of University policies or codes. You can either **delete and ignore junk e-mail** (this is the recommended approach) or contact the sender and ask to be removed from any mailing list they have - just as you would do with U.S. Postal mail.

Note that chain mail is a form of junk mail that is a violation of policy and can be reported. See the section on the Responsible Use of Electronic Communications policy for details on reporting chain mail.

- **Breaches of network etiquette**

Things like off-topic postings to lists and news groups, advertising by posting the same message to numerous lists (also known as "spamming"), rude or impolite behavior, heated arguments (or flame wars), and some forms of hate speech will often annoy others. Remember that the Internet spans the globe as well as numerous diverse cultures and societies. What is acceptable in one may be inappropriate in another. Keep in mind that it is easy to misunderstand electronic communications due to the lack of personal contact involved. You can avoid problems by "listening" for a while when you join a group. After you determine what is acceptable, then go ahead and post. If you participate in a discussion and someone posts off-topic, be polite in pointing out the mistake and do not assume it is deliberate.

Chatham is not in a position to control etiquette. When these sorts of problems come up, you should try to work them out with the other people involved, just as you do in other areas of your life. For more etiquette tips check out Netiquette Guidelines.

In some cases, rude behavior can cause disruptions. Any behavior that interferes with the ability of others to access or use a system is a violation of policy. See the section on Interfering with activities of others.

- **Hate speech**

Uncivil, antagonistic or derogatory speech that is disrespectful of classes of people is commonly referred to as hate speech. Although hate speech may be extremely offensive (particularly to members of the targeted group), posting hate speech does not generally constitute a violation of University policies or codes. This is because, especially as an educational institution, Chatham is committed to the protection of freedom of expression. In exceptional cases, however, the University may decide that hate speech directed to classes of individuals presents such a hostile environment that certain restrictive actions are warranted.

What is illegal under local, state and federal laws?

Any activity that is illegal is a violation of Chatham policy. Alleged violations will be referred to CSG. In addition, offenders may be investigated and/or prosecuted by the appropriate local, state or federal authorities.

- **Child pornography**

Child pornography, material that depicts minors in a sexually explicit way, is illegal. Under the federal child pornography statute (18 USC section 2252), anyone under the age of 18 is a minor. States also have child pornography statutes and the age of minority varies by state. **Knowingly uploading or downloading child pornography is a federal offense.** It is also illegal to advertise or seek the sale, exchange, reproduction or distribution of child pornography. Lewd exhibition of genitals can constitute sexual conduct and therefore, any graphic files containing images of naked children could violate the federal child pornography statute.

- **Distribution of pornography to minors**

The possession of non-obscene **adult** pornography on **non-University owned computer equipment** is legal and not in violation of University policy, but it is illegal to distribute it to minors.

- **Obscenity**

Obscenity is illegal. Virtually every state and municipality has a statute prohibiting the sale and distribution of obscenity, and the federal government prohibits its interstate transportation. The Supreme Court in *Miller v. California*, 413 U.S. 15, (1973), narrowed the permissible scope of obscenity statutes and applied this three part test to determine constitutionality: (a) whether the average person applying contemporary community standard would find the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes in a patently offensive way sexual conduct specifically defined in applicable state law; and (c) whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.

The contemporary community standard is historically the standard of the community in which the material exists. Many online activists argue that the contemporary community standard in cases that arise online ought to be determined by the online community. However, a federal prosecution of a California couple that offered a members-only bulletin board service, concentrating on pornography, resulted in a conviction of the California couple under the federal obscenity statute and Tennessee community standards because a customer in Tennessee had downloaded material over the Internet. See *United States v. Thomas*, 1996 U.S. App. LEXIS 1069 (6th Cir. Jan. 29, 1996).

- **Scams and pyramid schemes**

Beware of money-making "opportunities" on the Internet. A common scam is the pyramid scheme. You get an e-mail message with a subject like "MAKE MONEY FAST" and it instructs you to send money to the people on the list and then add your name to the bottom of the list and send it on to some number of people. At Chatham, this is considered chain mail, but it is also illegal under 18 U.S.C section 1302. The Federal Trade Commission provides information to help individuals identify scams and report them. Pyramid schemes that use US Postal mail to send money are considered mail fraud and can be reported to the USPS.

- **Copyright infringement**

Almost all forms of original expression that are fixed in a tangible medium are subject to copyright protection, even if no formal copyright notice is attached. Written text (including e-mail messages, news posts, and web pages), recorded sound, digital images, and computer software are some examples of works that can be copyrighted. Unless otherwise specified by contract, the employer generally holds the copyright for work done by an employee in the course of employment.

Copyright holders have many rights, including the right to reproduce, adapt, distribute, display, and perform their work. Reproducing, displaying or distributing copyrighted material without permission infringes on the copyright holder's rights. However, "fair use" applies in some cases. If a small amount of the work is used in a non-commercial situation and does not economically impact the copyright holder it may be considered fair use. For example, quoting some passages from a book in a report for a class assignment would be considered fair use. Linking to another web page from your web page is not usually considered infringement. However, copying some of the contents of another web page into yours or use of video clips without permission would likely be infringement.

- **Software piracy**

Unauthorized duplication, distribution or use of someone else's intellectual property,

including computer software, constitutes copyright infringement and is illegal and subject to both civil and criminal penalties. The ease of this behavior online causes many computer users to forget the seriousness of the offense. As a result of the substantial amounts of money the software industry loses each year from software piracy, the software companies enforce their rights through courts and by lobbying for and getting stiffer criminal penalties. It is a felony to reproduce or distribute ten illegal copies of copyrighted software with a total value of \$2,500 within a 180-day period. Penalties for a first time felony conviction of software piracy include a jail term of up to ten years and fines up to \$250,000.

- **Sound recording piracy**

Another form of copyright infringement is the unauthorized duplication and distribution of sound recordings. Online piracy is increasing as many people use the Internet to illegally distribute digital audio files (e.g. MP3 format). The Recording Industry Association of America (RIAA) monitors the Internet daily and scans for sites that contain music. They have been successful in getting the sound recordings removed from those sites. You can report violations to the RIAA directly (see section on Outside agencies).

Federal copyright law grants the copyright owner in a sound recording (typically, a record company) the exclusive right to reproduce, adapt, distribute and, in some cases, digitally transmit their sound recordings. Therefore, the following activities, if unauthorized by the copyright owner, may violate their rights under federal law:

- Making a copy of all or a portion of a sound recording onto a computer hard drive, server or other hardware used in connection with a web site or other online forum. This includes converting a sound recording into a file format (such as a .wav or mp3 file) and saving it to a hard drive or server;
- Transmitting a copy or otherwise permitting users to download sound recordings from a site or other forum; and/or
- Digitally transmitting to users, at their request, a particular sound recording chosen by or on behalf of the recipient.

If you reproduce or offer full-length sound recordings for download without the authorization of the copyright owner, you are in violation of federal copyright law and could face civil as well as criminal penalties. **Placing statements on your web site, such as "for demo purposes only" or that the sound files must be "deleted with 24 hours," does not prevent or extinguish this liability.** See "Copyright infringement" for more information on what is considered "fair use".

There are several entities you may need to contact before you can use recorded music online. First, you should understand that the copyright in a sound recording is distinct from the copyright in the recording's underlying musical composition. Thus, even if you have secured the necessary licenses for publicly performing musical compositions (from, for example, ASCAP, BMI and/or SESAC) or for making reproductions of musical compositions (from, for example, the Harry Fox Agency), these licenses only apply to the musical composition, not the sound recording. Licenses to utilize particular sound recordings must be secured from the sound recording copyright owners -- generally the record company that released the recording.

- **Federal computer security violations**

The primary federal statute regarding computer fraud 18 U.S.C section 1030 was

amended in October 1996 to protect computer and data integrity, confidentiality and availability. Examples of violations are:

- theft of information from computers belonging to financial institutions or federal agencies, or computers used in interstate commerce;
 - unauthorized access to government computers;
 - damage to systems or data (intentionally or recklessly);
 - trafficking in stolen passwords;
 - extortionate threats to damage computers;
 - computer viruses and worms.
- **Bomb threats and hoaxes**
It is illegal to send a message via e-mail that threatens other persons or property. While this might seem obvious, every year a number of individuals send what they believe are "hoax messages". Such messages may be investigated by federal authorities with the result that the senders end up with their names in the files of the FBI and/or CIA. This is not an exaggeration!

It also violates Chatham's policies and the Honor Code to send certain kinds of hoax messages (for example, April Fool's jokes that appear to be from a professor or some other college official). Such hoaxes constitute forgery and will be referred for appropriate disciplinary action.

Related sites

- [FindLaw Internet Legal Resources](http://www.fraud.com/) (http://www.fraud.com/)
- [The Virtual Magistrate](http://www.vmag.org/) (http://www.vmag.org/)
- [The Electronic Frontier Foundation](http://www.eff.org/) (http://www.eff.org/)
- [The Online Ombuds Office](http://www.odr.info/index.php) (http://www.odr.info/index.php)
- Chatham Honor Code