

Gretna Career College
Electronic Communications Policy
(Unauthorized Distribution of Copyrighted Materials)
Employee Notification

Introduction

Gretna Career College is committed to providing its employees, teachers and administrators, with access to advanced technologies to facilitate productivity in the workplace. Primary among these technologies is GCC's Electronic Communications Assets. However the use of these technologies requires all employees to use these assets properly. The information provided in this document serves as an employee tutorial for proper use of such equipment. Therefore, all employees are required to comply with the enumerated rules and admonitions.

Electronic Communications Due-Diligence Monitoring

It is important to understand that no employee utilizing GCC Electronic Communications Assets should have any expectation of absolute privacy in any Electronic Communications that he or she generates, stores, or uses on GCC Electronic Communications Assets since GCC reserves the right to monitor its Electronic Communications Assets as well as files existing on GCC's system for the purpose of ensuring compliance with GCC's Electronic Communications Assets policy. Additionally, government agencies and other outside persons or entities may have the legal right to request GCC records and/or information, including information that is stored electronically in GCC's computers or networks. GCC will always respond positively to such requests if they are legally and/or jurisdictionally valid. In addition to protecting the integrity of GCC communications assets, GCC has instituted measures to comply with the Digital Millennium Copyright Act (DMCA) and the Higher Education Opportunity Act (HEOA).

Copyright Infringement and Peer-to-Peer ("P2P") File Sharing Policy

Peer-to-peer, P2P, file sharing is not illegal. However, it is often used for unauthorized downloading and uploading of copyright-protected material such as music, movies, video games, computer software and photographs, which activities can trigger civil and criminal liabilities. Given that security flaws in P2P applications may provide ways to crash computers, access confidential information, distribute copyrighted material illegally, infect the entire network with viruses, and consume large amounts of bandwidth reserved for academic and administrative purposes, peer-to-peer file sharing (P2P) software is prohibited on the campus network at GCC. **For the aforementioned reasons, employee may not load or use P2P software on GCC's computers or networks.**

The proper use of GCC's Electronic Communications Assets goes beyond the use of P2P applications. Therefore listed below are additional prohibitions regarding the use of GCC computers and networks:

- Do not download computer games, shareware, or freeware (unauthorized use could subject you and GCC to liability for copyright infringement.)

Last updated on February 8, 2012

- Never distribute unauthorized copyright material including downloaded material acquired inside or outside of GCC.
- Do not load or use software from vendors distributed as shareware and freeware.
- Do not connect to Internet radio sites.
- Never use profanity or send jokes in emails or otherwise.
- Do not display, transmit, distribute, access, or make available information that could offend others based on race, religion, sexual orientation, age, political belief, gender, disability, or national origin.
- Never display, transmit, distribute, or make available information that could be abusive, obscene, defamatory, harassing, discriminatory, derogatory, offensive, or threatening.
- Do not interfere with or disrupt the normal operation of any GCC computer-based system or connecting network.
- Never use GCC Electronic Communications Assets to pursue personal profit or advancement of a non-GCC business interest.
- Do not engage in communications that are not directly related to your GCC responsibilities.
- Do not solicit persons on behalf of any organization, including soliciting money for any purpose (other than a GCC-approved solicitation).
- Never disclose confidential or proprietary information of GCC, its employees, customers, suppliers, or consultants without proper authorization.

Sanction for Violations of Electronic Communications Policy

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Gretna Career College imposes disciplinary actions for violations of its Electronic Communications Asset Policy on a case by case basis, and such sanctions may include suspension or dismissal. For the employee (which includes work study students), a first offense will result in a three day suspension without pay; a second offense may result in termination of employment with GCC. Violations to the Copyright Act may also invoke civil and criminal penalties. In general, if you are found liable for civil copyright infringement you may be ordered to pay either actual damages or “statutory” damages affixed at no less than \$750 and no more than \$30,000 per network infringed. For “willful” infringement, a court may award up to \$250,000 per work in fringed. In addition, a court can, at its discretion, assess other costs and attorney’s fee. Given such severe sanctions, GCC tends to view any instance of downloading and/or uploading copyright-protected materials by an employee as a violation subject to administrative sanctions up to and including dismissal.

Computer Etiquette Required When Using GCC Electronic Communications Assets

Last updated on February 8, 2012

Because it is the responsibility of all users to protect GCC Electronic Communications Assets and all confidential and proprietary information contain on GCC PCs and networks, all employee users should always act consistent with the following admonitions:

- Do not disclose any system-level login passwords to unauthorized parties.
- Do not reveal personally assigned passwords or user identifications (IDs) to others. If you forget your user id or password contact the local network administrator to have the password changed or the ID revoked.
- To prevent viral risks to the network, do not open email messages from unknown senders or download and install or attempt to install programs from unapproved sources.
- Do not disclose or transmit sensitive, proprietary, and confidential information over the Internet or voice-mail outside of GCC unless proper precautions are taken to ensure confidentiality, including approved encryption techniques.
- Do not encrypt sensitive, proprietary, and confidential information without prior permission from the local network administrator.
- Do not disclose GCC intellectual property, that is, price lists, marketing plans, software programs, advertising copy, or other materials that could be the subject of a patent, copyright, trademark, service-mark, or similar protection.
- Do not display non-confidential forms of intellectual property to large numbers of persons on internal or external websites or pages - unless authorized by a GCC administrator or network administrator. In addition, do not create a website or page that uses the GCC name, graphics, logos, or trademarks that would cause the viewer to believe that the website or page is sponsored by GCC or reflects the views of GCC.

Respect for the Rights of Others

As with other GCC policies and guidelines, we must always respect the rights of parties other than GCC when using GCC Electronic Communications Assets. These are powerful tools, and if used carelessly or wrongfully, may disclose confidential information or damage the assets of others, infringe on their intellectual property, harass people, or violate laws. At a minimum, we must all keep the following issues in mind when using GCC Electronic Communications Assets, and no employee should engage in the following activities when using GCC Electronic Communications Assets:

- View, send, upload, download, or store sexually explicit or pornographic materials, ethnic, or racially derogatory materials, or any other material that could be construed to be harassing or disparaging of others based on their gender, race, disabilities, sexual orientation, age, national origin, religious, or political beliefs since such acts may potentially harass or intimidate of others.
- Transfer computer software or technical documents by electronic mail or upload software onto the Internet in violation of the export laws of the United States or other countries. (Only a GCC administrator or network administrator can approve the uploading of any software or technical documents to the Internet.)
- Attempt to circumvent access safeguards by attempting to gain access to the computers, networks, passwords, accounts, files, or data of others. (All authorized access problems should be referred to a network administrator.)

Last updated on February 8, 2012

- Harass other users with unwelcomed transmissions in the form of audio, video, software programs, or computer instructions that could delete, damage, harm, destroy, or in any way affect the data, software, computers, or electronic assets of others (such as computer viruses).

Due Diligence Reporting

Finally, if you become aware of a situation where you believe your legal and/or ethical responsibilities are being violated or you feel that you are being pressured to violate the law or your ethical responsibilities with regard to GCC's Electronic Communications policy, it is your personal responsibility to communicate such concerns to your GCC supervisor.

[For full Gretna Career College Electronic Communications Policy, click here >>](#)

GCC Communications Policy Signature Page

I have read and understood all the rules, warnings, and procedures which constitute GCC's Electronic Communications Policy, and also understand that violations of this policy are considered serious and could result in disciplinary action up to possible termination.

The policy's primary purposes are to prevent violations of the Digital Millennium Copyright Act (DMCA), the Higher Education Opportunity Act (HEOA), and to safeguard GCC Communications Assets.

In accordance with GCC policy, there is a strict prohibition against the sharing of login IDs and/or passwords – no exceptions. If someone does use your ID or password, you will be held accountable for its usage.

I hereby agree to and will abide by all directives stated in GCC's Electronic Communications Policy, and will not reveal my assigned login ID and password to anyone.

Signature: _____ Date: _____