

Gretna Career College
Electronic Communications Policy
(Unauthorized Distribution of Copyrighted Material)

Introduction

Gretna Career College (hereinafter “GCC”) is committed to the use of advanced technologies in its business operations. These powerful tools, provided for business and educational purposes, expand the information available to us and enhance our ability to communicate with each other, our business partners, vendors, and customers. These tools shall be called Electronic Communications Assets and include electronic computers, printers, mail (E-mail) applications, LANs, WANs, on-line services, and the Internal Web. There are some serious risks associated with misuse of GCC’s Electronic Communications Assets. As a result, all users of such assets shall be governed by the policy herein established and are obliged to comply with the rules, admonitions, and prohibitions embodied in this policy. In addition to protecting the integrity of GCC Electronic Communications Assets, GCC has instituted measures to comply with the Digital Millennium Copyright Act (DMCA) and the Higher Education Opportunity Act (HEOA). Since complying with these mandates requires periodic overt monitoring of activities performed by users utilizing GCC’s Electronic Communications Assets, students are required to sign an agreement during their New Student Orientation session which makes them aware of their diminished privacy.

Basic Rules for Electronic Communications

GCC’s Electronic Communications Assets Policy is the written plan implemented to protect GCC’s communications assets from damage and to combat unauthorized downloading and distribution of copyrighted materials on its computers and networks. Such measures consist of software, hardware and disclosed warnings to students and employees which foster proper use and discourage or prevent improper use of GCC PCs and networks and attached devices.

Protection Measures (Access Control)

Access to computers on the GCC network is managed by Directory Services software which provides access and prevents unauthorized access based on a hierarchy of designated privileges assigned to all users of GCC computers and networks. The hierarchy of rights provides and limits access to directories on the GCC system. As a result, users are grouped into classes and cannot access information to which they do not have overt privilege. All access is realized through assigned usernames and passwords assigned by a network administrator or designated employee.

In addition, firewalls have been established and will be maintained that block the ports of Peer-to-Peer (P2P), software, which is explicitly not permitted on any GCC computer or network. Through such methods of technical enforcement, GCC strives to preserve the integrity of its network at all times. Furthermore, any computer found to be running P2P software will be blocked from campus network access until the software has been removed from the computer. A Systems Administrator in the Information Technology division must verify removal of the P2P software before network access is restored.

Monitoring Measures

It is important to understand that no one utilizing GCC Electronic Communications Assets should have any expectation of absolute privacy in any Electronic Communications generated or stored on GCC Electronic Communications Assets since periodic inspection and/or monitoring of GCC computers and networks is required to protect such computers and networks from unauthorized use and/or security compromises. GCC, therefore, actively exerts its right to inspect its Electronic Communications Assets and files existing on GCC's system for the purpose of ensuring compliance with its Electronic Communications Assets Policy and protecting its significant investments in same. Such periodic incidents of inspection will be conducted by the network administrator, and to ensure proper usage of GCC's Electronic Communications Assets, such random periodic reviews will be reviewed by the Campus Director, at a minimum, every 3 months or as otherwise indicated.

Compliance with Outside Agencies

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.

DISCLOSURE WARNINGS AND MECHANISMS FOR EDUCATING AND INFORMING THE COMMUNITY

GCC provides written notification to students during New Student Orientation delineating proper use of its networked computer system as well as informing them that inspections of the results of their activity are performed periodically to ensure proper conduct on GCC systems and to dispel any expectation of absolute privacy when utilizing GCC communications assets. In addition, the GCC student catalog provides an additional brief description to doubly encourage students about the prohibition against improper conduct on its networks. Relevant documents may also be made available to students and administrators on topical bulletin boards.

The content of the aforementioned written disclosures to students and employees includes but is not necessarily limited to the relevant items below:

- Do not download computer games, shareware, or freeware (unauthorized use could subject GCC to liability for copyright infringement).
- Never distribute unauthorized copyrighted material including downloaded material acquired on GCC's PCs or networks or outside of GCC or use P2P file sharing software on GCC's PCs or networks. In doing so, the student or employee may be subject to civil and criminal liabilities as well as possible suspension from GCC.
- Many legitimate vendors distribute both shareware and freeware. However, using the appropriate procurement channels will protect GCC's assets.
- Do not connect to Internet radio sites. These sites cause unnecessary burden on the networks, causing performance issues for all other systems connected to the network.

- Never use profanity or send jokes.
- 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).
- Do not engage in any activity otherwise prohibited by any GCC policy, rule, or guideline.
- Never disclose confidential or proprietary information of GCC, its employees, customers, suppliers, or consultants without proper authorization.

COPYRIGHT INFRINGEMENT AND PEER-TO-PEER (“P2P”) FILE SHARING POLICY

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. As a result, students and employees are informed of the prohibition on using P2P software in an emphasized fashion, that is, in a separate paragraph in their disclosure document.

Due Diligence Reporting

To encourage proactive due-diligence, students and employees are informed that if they become aware of any situation where they believe their legal and/or ethical responsibilities are being violated or feel that they are being pressured to violate the law or their ethical responsibilities with regard to GCC’s Electronic Communications policy, they should immediately communicate such concerns to their teachers or trusted GCC administrator or network administrator.

SANCTIONS FOR VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS POLICY AND FOR VIOLATION OF FEDERAL COPYRIGHT LAWS

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. Obviating such infringement is a salient goal of GCC in the management of its PCs and networks.

Penalties for copyright infringement include civil and criminal penalties. In general, if a student is found liable for civil copyright infringement he or she 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 \$150,000 per work infringed. In addition, a court can, at its discretion, assess other costs and attorney’s fee. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to \$250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQs at www.copyright.gov/help/faq.

GCC SANCTIONS

GCC views any instance of downloading and/or uploading copyright-protected materials by a student or employee as a violation subject to administrative sanctions up to and including dismissal.

Therefore, also included in the aforementioned student and employee disclosure documents are descriptions of the consequences for discovered instances of improper conduct on GCC’s PCs and networks including but not necessarily limited to the sanctions below.

Gretna Career College imposes disciplinary actions for violations of its Electronic Communications Asset Policy U.S. on a case by case basis, and such sanctions may include suspension or dismissal. However, generally for the student, a first offense will result in a loss of or restricted privileges in using any GCC computer for six months; a second offense will result in the expulsion of the student from GCC. For the employee (which includes work study students), a first offense will result in a three day suspension without pay; a second offense will result in termination of employment with GCC.

General Principles for Productive and Safe Use of GCC Electronic Communications Assets

Because it is the responsibility of all users to protect GCC Electronic Communications Assets and all confidential and proprietary information contained on GCC PCs and networks, all student and employee users are provided with relevant disclosures also embodying but not limited to 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. In the event security is breached on any account, 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 E-mail messages from unknown senders or download and install or attempt to install programs from unapproved sources. It is your responsibility to take all appropriate measures to prevent viruses.
- Do not use GCC Electronic Communications Assets to improperly disclose proprietary or confidential information of GCC, our employees, students, customers, suppliers, or consultants – in general to any unauthorized parties.
- 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 all such admonitions below are also disclosed to students and employees in the aforementioned disclosure documents.

All GCC Electronic Communications Asset users should never do the following:

- 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 are potentially form of harassment or intimidation 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.

- 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).

LAST UPDATED FEBRUARY 10, 2012