View/Print Document: AR 2240

Back | Main Index | Series Index | Next

Glendale Community College District 2240

Administrative Regulation

Using Information Technology Resources at Glendale Community College

Part I: Introduction

Glendale College is an institution of higher learning dedicated to the transmission of knowledge and to the intellectual and personal development of its students. It is for the realization of these purposes that it maintains an extensive array of information technology resources, which it places at the disposal of its entire College community. Such resources include, but are not limited to, the central computing services, the campus-wide network, the various computer labs, electronic mail, Internet access, voice mail, and other related equipment and services. These resources are extremely valuable and provide access to sensitive data and to extensive external networks. Consequently, it is important for all users to behave in a responsible, ethical and legal manner. In general, appropriate use means respecting the rights of other computer users, the integrity of the physical facilities, and all pertinent license and contractual agreements. This document establishes more specific guidelines for the use of all College computing resources.

These guidelines apply to all computing resources owned or managed by GCC or using its network, and to all the users of these resources, including but not limited to Glendale's faculty, staff, students, and guests, and individuals or organizations accessing external network services, such as the Internet, via Glendale's computing facilities. These guidelines also apply to all computing resources not owned by GCC, which are located in GCC facilities. These non-college owned computing resources should be clearly marked as such and are the sole responsibility of the owner. GCC can assume no liability for these devices nor support the operation of these computing resources. Individual departments may have additional policies regarding their computing equipment: please contact them for more information about these policies.

The College has established specific procedures to be followed when abuse of computing resources has allegedly occurred. These procedures are defined in Appendix A. Questions regarding policy, interpretation of policy, or special problems or needs should be directed to the Dean of Information Technology Services (ITS). It is the sole responsibility of the user to be familiar with this policy and its provisions.

This document has been adapted from the guidelines for the use of computing resources at Brown University. It has been prepared by the Campus-wide Computer Coordinating Committee (CCCC), and approved by the Campus Executive Committee on 3/12/02.

Part II: Guidelines for appropriate computing behavior

The following list, while not exhaustive, provides some specific guidelines for responsible and ethical behavior:

1. Use only the computers, computer accounts and computer files for which you have authorization. Do not use another individual's account, or attempt to capture or guess other users' passwords. Users are individually responsible for all use of resources assigned to them; therefore, sharing of accounts is prohibited.

2. Obey established guidelines for any computers or networks used both inside and outside the College. For example, individuals accessing off-campus computers via external networks must abide by the policies established by the owners of those computers as well as policies governing use of those networks.

3. Do not attempt to access restricted portions of the network, an operating system, security software, or accounting software unless authorized by the appropriate College administrator or owner. Breaking into computers is explicitly a violation of Internet rules of conduct and of the law, no matter how weak the protection is on those computers. Tapping into telephone or network lines is a clear violation of College policy.

4. Abide by all state and federal laws (Appendix B provides links to some relevant California and federal laws)

5. Respect the privacy and personal rights of others. Do not access or copy another user's electronic mail, data, programs, or other files without permission. Guidelines in the College catalog regarding academic honesty apply to course work completed with computers just as they do to other types of course work.

6. Abide by all applicable copyright laws and licenses. It is against both College policies and the law to copy software that has not been placed in the public domain or distributed as "freeware." "Shareware" users are expected to abide by the requirements of the shareware agreement. Respect the copyright law as it applies to images, texts and sounds in the production of electronic information.

The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement. The unauthorized use or distribution of copyrighted works (including Web page graphics, sound files, trademarks and logos) is prohibited and may provide the basis for disciplinary action, civil litigation and criminal prosecution.

7. Use appropriate standards of civility when using computing systems to communicate with other individuals. When sending messages to other users, identify yourself as the sender unless you are acting as a proxy with permission to use another's name. Always seek to maintain an environment conducive to learning. Using Glendale's computing resources to harass or threaten other individuals deliberately is explicitly prohibited.

8. Be sensitive to the needs of others, avoid wasteful activities and use only your fair share of computing resources. For example, users of shared resources, such as the central computer, should use these facilities for only the most essential tasks during periods of peak demand. Broadcasting non-sanctioned messages to large numbers of individuals and sending chain letters are examples of activities that cause network congestion and interfere with the work of others, and thus are not allowed.

9. Treat computing resources and electronic information as a valuable College resource. Protect your data and the systems you use. For example, back up your files regularly. Set a password that is not easily guessed and change it regularly. Make sure you understand the access privileges you have set for your files and computer system. Do not destroy or damage any computing equipment, networks or software. The willful introduction of computer viruses, worms, Trojan horses or any other infection into the GCC computing environment or into other computing environments via Glendale's network violates College standards and regulations.

10. Use Glendale's computing facilities and services for College related work. Activities that would jeopardize the College's tax-exempt status such as improper political activities or activities for personal gain are prohibited (see part III, sections 6 and 7).

11. Stay informed about the computing environment. The computing environment is continually evolving, as new products are introduced and others become obsolete. Services change as the number and needs of users' change. Glendale publishes information in a variety of ways, including Web pages, electronic messaging, general news items that users are prompted to read, news groups associated with particular compilers or software packages, on-line documents about software, policy and procedures, and in some cases, e-mail to individuals. Users are responsible for staying informed about changes in the computing environment and are expected to adapt to these changes.

12. Be wary of installing or downloading personal software on college equipment. Such operations will be at your own risk and may result in loss of data and/or other problems. ITS is not responsible for supporting personal software or for solving problems created by such software. Students are prohibited from installing or downloading personal software on college equipment.

Part III: Users' rights and responsibilities

1. Access to computing resources

Central computing services: Faculty and College employees may obtain an ID for use with the central computing services for activities related to instruction or College administration. Individuals not at Glendale may, under some circumstances, also obtain a user account. Contact the Help Desk within Information Technology Services for detailed information about obtaining and using central computing facility accounts.

Other IT computing resources: Most of Glendale's computing facilities and services are available to members of the College community. For more detailed information about access to any facility or service, contact Information Technology Services or the appropriate department head or division chair.

2. Data security and integrity

Owners of data are responsible for the backup of their files. ITS will provide centralized backup solutions for mission critical data and will attempt to provide backup services for departments and services as budget allows. However, since ITS does not provide the same level of protection or file restoration for servers not located in ITS, it is especially important that users back up their files and use all available means to protect their data on departmental systems.

ITS provides reasonable security against intrusion and damage to files stored on the central computing services. However, neither the College nor any ITS staff can be held accountable for unauthorized access by other users, nor can they guarantee protection against media failure, fire, floods, etc.

Users should use all available methods to ensure the physical security of their computers and to protect their files, including the frequent changing of their passwords and storing back-up copies of information off site. In addition, users are regularly notified of potential virus threats and are required to follow instructions in such cases. They are also required to scan routinely for infections. In the event that data have been corrupted as a result of intrusion, ITS and Campus Police should be notified immediately. Upon request, ITS staff will assist in implementing procedures to maximize security.

In an emergency, ITS managers have the right to disconnect temporarily a user if network or mission critical systems are endangered.

3. Privacy

User account and files: Although not legally required to do so, ITS respects the privacy of all users. Members of ITS staff are forbidden to log on to a user account or to access a user's files unless the user gives explicit permission (for example, by setting file access privileges).

Exceptions to this privacy policy are made, however, under specific conditions. One such condition is if a user is suspected of causing disruption or using unreasonable bandwidth on the network or other shared services. Another condition is a suspected

violation of state or federal law. In these instances, if the user is an employee of the College, the Dean of ITS, with the concurrence of the President or the Executive Vice-President of the College, must be convinced that there is sufficient cause to review a file(s) before those files can be searched without the user's permission. If the user is a student, the same procedures apply, except that the Dean of ITS or the manager of the local area network can decide alone if there is sufficient grounds to search the files of the suspected user.

Before logging onto a user's account or accessing a user's private files, a reasonable attempt will be made to contact the user to inform him or her that ITS will access the files. If that is not possible, the Dean of ITS or an authorized agent will view the files for the suspected violation and will inform the user afterward that the files have been reviewed. Information obtained in this manner is admissible in legal proceedings or in a College Judicial Board hearing. In accepting a user account, the user agrees to this policy.

If an employee feels that his/her privacy has been violated by a member of ITS, he/she may request that the CCCC investigate the matter. Upon reception of the request the CCCC shall form an independent committee and proceed with the investigation. The results shall be forwarded to Human Resources Complaint Review Procedure as set forth in Administrative Regulation 4050. A request can be brought up to the CCCC through any of its members.

If a student feels that his/her privacy has been violated by a College employee, he/she may file a complaint with the Dean of Student Affairs who will then follow the standard procedure for the resolution of student complaints.

Electronic mail: Electronic mail is subject to the privacy policies explained above for ordinary user accounts and files. However, users should not expect total privacy of electronic mail (e-mail). ITS staff may see the contents of e-mail due to serious addressing errors or as a result of maintaining the e-mail system. In those cases where ITS staff do see the contents of private e-mail, they are required to keep the contents confidential. Users should also be aware that the current design of the Internet is such that the privacy of e-mail that leaves Glendale cannot be guaranteed.

When a user's affiliation with Glendale ends, e-mail subsequently received at Glendale that is addressed to the former user will either be returned to the sender or, if appropriate, forwarded to an address specified by the former user. ITS also reserves the right to close accounts that have been dormant for six months or more.

Users are reminded that e-mail is easily redistributed and may be read by people beyond the original recipient list. Care should be taken in phrasing e-mail given the uncertainty of readership.

4. Freedom of speech

The College recognizes and respects the rights of users to freedom of speech. Such rights, however, are not absolute. Speech which is fraudulent, libelous, obscene, harassing or threatening is not permitted under state or federal law. Please refer to

Appendix B for links to some relevant California and federal laws.

5. Ownership of copyright for materials developed with Glendale's resources

Ownership of copyright eligible property is determined by negotiated agreement between the College and the Glendale College Guild or the CSEA. Please contact the Guild or the CSEA for further information.

6. Personal financial gain

Because of the tax-exempt status of the College, the use of its computing resources for personal financial gain is prohibited. Employees, however, are allowed to use these resources to prepare material for use in their College work even though such material may later be copyrighted (see section 5 above).

7. Political activity

In general, political activity in the form of providing information or educating the public is permitted on a community college campus. College personnel and students are free to express their political views provided it is made clear that they are not speaking for or in the name of the institution. Campus organizations and individuals may use the computing resources of the College to publicize political forums or discussions, but may not use them to endorse, raise money for or otherwise promote a candidate for public office, or a political party, organization or lobby. For further information please refer to Appendix B for links to some relevant California and federal laws, or to Glendale Community College Board Policy sections 1410, 5220, 5420, 5440 and 6132.

8. Responsibility for errors in software, hardware, and consulting

Glendale makes every effort to maintain an error-free hardware and software environment for users and to ensure that the computing staff is properly trained. Nevertheless, it is impossible to ensure that hardware or system software errors will not occur or that staff will always give correct advice. Glendale Community College presents no warranty, either expressly stated or implied, for the services provided. Damages resulting directly and indirectly from the use of these resources are the responsibility of the user.

However, at the request of the user, when hardware, software, or consulting errors are determined to have occurred on central computing services, ITS will make a reasonable attempt to recover files to their state prior to the failure, at no cost to the user. As part of maintaining the software environment, ITS applies vendor-supplied or locally developed fixes as appropriate when problems are identified. Given that vendors may be involved and that staff resources are finite, no guarantee can be made as to how long it may take to fix an error once it has been identified. When software errors are considered major problems or could produce inaccurate results, users will be notified as soon as possible using appropriate electronic and/or other media.

9. Changes in the computing environment

When significant changes in hardware, software or procedures are planned, ITS will notify the College community through electronic and other media to ensure that all users have enough time to prepare for the changes and to voice any concerns that they might have.

Part IV: Use of Non-Glendale Owned Equipment on the College's Network

Equipment which is purchased using personal funds or which remains the property of an agency by grant or contract may use the resources of the Glendale network providing the following guidelines are observed:

1. Owners, or in the case of grant/contract equipment, the contractual administrator (s), must assume responsibility for the use of their equipment; usage must conform to the standards for Glendale owned equipment

2. Owners, or in the case of grant/contract equipment, the contractual administrator (s), must ensure that the use of their equipment on the Glendale network does not to place an inordinate burden on the system. If traffic is unduly impeded by its use, they must either discontinue the service or find an external service provider.

3. Owners, or in the case of grant/contract equipment, the contractual administrator (s), must not permit access to the network or any of its services that would not otherwise have been granted through official College procedures.

4. Non-Glendale owned machines on the Glendale network may not be used for profit, personal gain, political campaigning, or in any manner that would compromise the College's non-profit educational status.

5. Non-Glendale owned machines on Glendale's network may not be used in support of any illegal activity or any activity which violates GCC policy. Examples of this include, but are not limited to, illegally distributing licensed software, using equipment in support of a crime, or sending harassing mail. The College will respond to known instances of this type of activity using disciplinary procedures which could include notification of local and federal police agencies.

To ensure a high level of service to its users, the College monitors traffic on its network. It may also monitor traffic to/from a particular non Glendale owned machine if there is reason to believe that there is activity which could impact the College. The procedures outlined in Appendix A will be used in cases of suspected violations of these guidelines.

Adopted: 3/12/02

Appendix A

Procedures for Handling Alleged Abuse of Computer Systems

1. Upon receipt of a complaint alleging abuse of computing resources as defined in this document, the Dean of ITS shall make a determination as to whether there is enough cause to initiate judicial proceedings. As part of this determination, the Dean may authorize the review of file(s) without the user's permission as described in Part III, section 3.

2. If there appears to be cause, the Dean of ITS shall attempt to contact the alleged violator via a combination of telephone, e-mail and written correspondence informing the individual of the alleged offense. This correspondence shall request a personal meeting between the alleged offending party, and the Dean of ITS (or a designated agent). If the alleged violator fails to respond to these attempts within three working days, the Dean of ITS will automatically initiate further proceedings.

3. If the meeting identified in section 2 above takes place, the Dean shall determine whether the incident and circumstances involved warrant referral of the individual to the appropriate judicial process. This determination will be made upon input from all concerned parties, and will depend on the seriousness of the alleged violation, and on the extent to which the individual demonstrates an understanding of the problem and appears unlikely to commit future violations.

4. If this meeting provides positive results and the Dean is satisfied that the violation has been fully understood and is unlikely to recur, he/she may declare the matter closed. If the results of the meeting are not satisfying, the Dean shall refer the individual to the appropriate judicial proceedings. Such proceedings ould include those specified in Board Policy section 1330 Complaints Concerning College), 4050 (Employee Complaints), 5100 (Students' Grievance Procedures), 5420 (Standards of Student Conduct and Disciplinary Action) or any other pertinent Board Policy provisions.

5. Access to the College computing resources may be suspended at the discretion of the Dean of ITS based upon the severity of the offense, whether the College is at risk of litigation, whether the alleged violation reflects a repeat offense, an endangerment of the system, or other cause which is perceived to directly harm the computing environment at GCC. In any case where suspension has occurred, all procedures identified in this document are immediately initiated. If suspension of access has occurred, the alleged violator may at any time request that his/her access be reinstated pending final resolution of the matter. This request must be addressed in writing to the person in charge of the appropriate judicial procedure who will then decide on its merit in consultation with the Dean of ITS.

6. The judgment resulting from the appropriate judicial process shall be final, and should include a recommendation as to the extent and timing of access to the system.

Adopted: 3/12/02

Appendix B

Links to some relevant state and federal laws

Note: There is growing international attention to legal prohibition against unauthorized access to computer systems, and several countries have passed legislation that addresses the area. In the United States, the Computer Fraud and Abuse Act of 1986, Title 18 U.S.C. section 1030 makes it a crime, in certain situations, to access a Federal interest computer (federal government computers, financial institution computers, and a computer which is one of two or more computers used in committing the offense, not all of which are located in the same state) without authorization. Most of the 50 states have similar laws regarding unauthorized access or other misuse of computer technology and violators can be prosecuted in the state or country