CAMPUSWIDE COMPUTER COORDINATING COMMITTEE

MEETING AGENDA

January 21, 2010

CR 137

12:00 p.m.

CALL TO ORDER

APPROVAL OF MINUTES from November 19, 2009.

OLD BUSINESS

1. Technology Plan?

NEW BUSINESS

1. CCLC Recommendation to Update BP 2240 and AR 2240 for Accreditation Purposes
2. GCC Student Email Policy
3. Use of Signature Quotes in Email (Mary Mirch)
4. Faculty/Staff Computer Data Backup (Tom Voden)
5. Computer Standby Feature for Power Savings (Mike Reed)

OTHER

ADJOURNMENT

UNADOPTED

CAMPUSWIDE COMPUTER COORDINATING COMMITTEE
MEETING MINUTES
November 19, 2009
CR 137

Present: Reed Anderson (Resource), Sevada Avakian (CSEA), K.C. Camp (Faculty), Susan Courtey (Resource), Dennis Doyle (Guild), Michael Dulay (Faculty), Bill Elbettar (CSEA), Kathy Flynn (Senate), Shereen Fogel-Allison (Admin), Pat Hurley (Resource), Brenda Jones (Resource), Edward Karpp (Resource), Mary Mirch (Admin), Simon Mirzayan (CSEA), Amir Nour (Admin), Arnel Pascua (Chair), Jewel Price (Admin), Susan Roberts (CSEA), Gretchen Smart (Resource), Kaleung Tsou (Resource), Thomas Voden (Faculty), Antonio Zarate (ASGCC),

Absent: Ed Bugayong (Resource), David O'Donnell (Resource), Alfred Ramirez (Admin), Daniel Ramirez (ASGCC), Mary Stone (Resource),

Guests: Frankie Strong, Poorna Pal, Michael Ritterbrown

Call to Order: The meeting was called to order by Chair, Arnel Pascua, at approximately 12:10 p.m.

Approval of Minutes:

It was MSC that the minutes from October 15, 2009 be approved.
(2 members abstained).

Old Business:

1. Anti-Spam Solution:

   - The college's contract with Google (Postini) Is due to expire within a year. The college has been testing Ironport as an alternate anti-spam solution. After testing of both products, a decision needs to be made to either renew with Google (Postini) or switch to Ironport.

     - *It was MSC that the college renew with Google (Postini) for its anti-spam solution.*
       (Two members abstained).

New Business:

2. Governance Best Practices:

- Guests Poorna Pal and Frankie Strong (on behalf of the Governance Review Committee) made a presented a mini-Governance workshop.
- Discussion items included: Duties of Governance Chairs and Members, Parliamentary procedures, Review of committee mission statement and membership, Overview of how motions are handled and the Mission Statement of the college's Governance Policy.

Other:

- The December CCCC meeting is scheduled during the week of finals. There was discussion to either have the next meeting on an alternate date in December or wait until January 2010.

➢ *It was MSC that the next meeting would be held in January 2010 instead of December 13.*
(One member abstained).

Meeting adjourned: at approximately 1:05 p.m.

Next Meeting Date: January 21, 2010

Returning Items:

1. Technology Plan
2. Use of Signature Quotes in email (Mary Mirch)
3. Faculty/Staff Computer Data Backup (Tom Voden)
4. Computer Standby Feature for Power Savings (Mike Reed)

Recorded by: Gordon Lui

View/Print Document: BP 2240

Back | Main Index | Series Index | Next

Glendale Community College District
2240

Board Policy

Computer and Communications Technology Use

Glendale Community College encourages the use of computer and communications technology, including computer networking, in order to enhance both the District's operation and the learning environment for students, faculty, and staff. In order to prevent the misuse of such technology, the College shall develop and regularly update procedures related to campus computing, networks, dial-up access, and all other such electronic communication systems.

Adopted: 5/15/95

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

BP 3720 Computer and Network Use

Reference:

Education Code Section 70902; 17 U.S.C. Section 101 et seq.; Penal Code Section 502, Cal. Const., Art. 1 Section 1; Government Code Section 3543.1(b)

Employees and students who use District computers and networks and the information they contain, and related resources have a responsibility not to abuse those resources and to respect the rights of others. The *Superintendent/President* shall establish procedures that provide guidelines to students and staff for the appropriate use of information technologies. The procedures shall include that users must respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other computer users.

See Administrative Procedures 3720.

AP 3720 Computer and Network Use

Reference:

17 U.S.C. Section 101 et seq.; Penal Code Section 502, Cal. Const., Art. 1 Section 1; Government Code Section 3543.1(b); Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

Note: This procedure is legally advised. Local practice may be inserted. The following is an illustrative example:

The District Computer and Network systems are the sole property of *[name of District]*. They may not be used by any person without the proper authorization of the District. The Computer and Network systems are for District instructional and work related purposes only.

Comment [a1]: See AR2240 page 3, item 10

This procedure applies to all District students, faculty and staff and to others granted use of District information resources. This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes personal computers, workstations, mainframes, minicomputers, and associated peripherals, software and information resources, regardless of whether used for administration, research, teaching or other purposes.

Comment [a2]: See AR2240 page 1, 2nd paragraph

Conditions of Use. Individual units within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines and/or restrictions.

Comment [a3]: See AR 2240 page 1, 2nd paragraph, last sentence

Legal Process. This procedure exists within the framework of the District Board Policy and state and federal laws. A user of District information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action.

Comment [a4]: See AR2240 last paragraph on page 1 and Appendix A

Copyrights and Licenses. Computer users must respect copyrights and licenses to software and other on-line information.

Copying - Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

Number of Simultaneous Users - The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

Copyrights - In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

Comment [a5]: See AR2240 page 2, item 6

Integrity of Information Resources. Computer users must respect the integrity of computer-based information resources.

Comment [a6]: See AR2240 page 2, item 3

Modification or Removal of Equipment - Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

Unauthorized Use - Computer users must not interfere with others access and use of the District computers. This includes but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs, running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, equipment, software or computer files.

Unauthorized Programs - Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

Unauthorized Access. Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

Abuse of Computing Privileges - Users of District information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the District. For example, abuse of the networks to which the District belongs or the computers at other sites connected to those networks will be treated as an abuse of District computing privileges.

Reporting Problems - Any defects discovered in system accounting or system security must be reported promptly to the appropriate system administrator so that steps can be taken to investigate and solve the problem.

Password Protection - A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.

Comment [a7]: See AR2240 page 2, items 1-5

Usage. Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of District procedure and may violate applicable law.

Comment [a8]: See AR2240 page 2, item 5

Unlawful Messages - Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, state or other law or District policy, or which constitute the unauthorized release of confidential information.

Comment [a9]: See AR2240 page 3, item 7

Commercial Usage - Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below). Some public discussion groups have been designated for selling items by *[insert names of groups, if any]* and may be used appropriately, according to the stated purpose of the group(s).

Comment [a10]: See AR2240 page 6, item 6

Information Belonging to Others - Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.

Rights of Individuals - Users must not release any individual's (student, faculty, and staff) personal information to anyone without proper authorization.

Comment [a11]: See AR2240 page 2, items 1-5

User identification - Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.

Comment [a12]: See AR2240 page 3, item 7

Political, Personal and Commercial Use - The District is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters.

Political Use - District information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws.

Personal Use - District information resources should not be used for personal activities not related to appropriate District functions, except in a purely incidental manner.

Commercial Use - District information resources should not be used for commercial purposes. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not appropriate within those domains.

Comment [a13]: See AR2240 page 6, items 6-7

Nondiscrimination. All users have the right to be free from any conduct connected with the use of *[name of district]* network and computer resources which discriminates against any person on the basis of *[insert list from Board Policy on nondiscrimination]*. No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Comment [a14]: See AR2240 page 5, item 4

Disclosure

No Expectation of Privacy - The District reserves the right to monitor all use of the District network and computer to assure compliance with these policies. Users should be aware that they have no expectation of privacy in the use of the District network and computer resources. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the system.

Possibility of Disclosure - Users must be aware of the possibility of unintended disclosure of communications.

Retrieval - It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.

Public Records - The California Public Records Act (Government Code Sections 6250 *et seq.*) includes computer transmissions in the definition of "public record" and nonexempt communications made on the District network and computer must be disclosed if requested by a member of the public.

Litigation - Computer transmissions and electronically stored information may be discoverable in litigation.

Dissemination and User Acknowledgment

All users shall be provided copies of these procedures and be directed to familiarize themselves with them.

A "pop-up" screen addressing the e-mail portions of these procedures shall be installed on all e-mail systems. The "pop-up" screen shall appear prior to accessing the e-mail network. Users shall sign and date the acknowledgment and waiver included in this procedure stating that they have read and understand this procedure, and will comply with it. This acknowledgment and waiver shall be in the form as follows:

Computer and Network Use Agreement (Sample Language)

I have received and read a copy of the District Computer and Network Use Procedures and this Agreement dated, _____, and recognize and understand the guidelines. I agree to abide by the standards set in the Procedures for the duration of my employment and/or

enrollment. I am aware that violations of this Computer and Network Usage Procedure may subject me to disciplinary action, including but not limited to revocation of my network account up to and including prosecution for violation of State and/or Federal law.

Comment [a15]: HR disseminates these procedures upon employee's hiring and obtains signature using a tear-out slip on the back page of the procedure booklet.

GCC Student Email Procedures

Deleted: Policy

INTRODUCTION

Electronic mail or "email" is considered an official method of communication to the students at Glendale Community College because it delivers information in a convenient, timely, and cost effective manner.

POLICY STATEMENT

GCC assigned student email accounts shall be one of the college's official means of communication with all enrolled students. Students are responsible for all information sent to them via their college assigned email account. If a student chooses to forward their college email account, he or she is responsible for all information, including attachments, sent to any other email account.

To assure all students access to this important form of communication, GCC will provide a college email account to each enrolled student. The primary purpose of these accounts is to ensure a standardized channel for faculty and staff to communicate with students as needed. Official college communications sent to all students will include reminders of important dates such as deadlines to pay tuition and fees, apply for graduation, etc. Students are responsible for checking their official student email regularly and reading college-related communications. In addition, it is Glendale Community College's policy to only respond to student emails originating from the assigned GCC student e-mail address.

Please Note: *No confidential information will be sent to students via email. Students may be directed to the college portal via email with issues regarding any actions (notification of probation, suspension, disciplinary action, etc.). (Please also refer to the Privacy section on page 4 of this document.)*

STUDENT OBLIGATIONS

Implementation of this student email policy places certain obligations on each student.

a) Students understand they have been given a college email account by virtue of attending GCC.
b) Students shall adhere to proper and appropriate use of email in accordance with these procedures.
c) Students shall responsibly manage their email account on a frequent and consistent basis (i.e. archiving attachments, deleting old messages, etc.).
d) Students understand that in some circumstances, the college will have to supplement electronic communication with traditional mail.

Deleted: the GCC email policy

COLLEGE OBLIGATIONS

Implementation of this student email policy places certain obligations on the college and employees.

a) The college will never lease or sell a student email address to any advertisers.
b) The college will provide access to computers with Internet capabilities on campus (e.g. open computer labs).
c) Email shall not be the sole method for notification of any legal action.
d) E-mail messages sent through mailing lists must abide by the college's Mass Communications Policy.

GUIDELINES

The student email policies provide guidelines regarding the following aspects of email as an official means of communication with students:

1. Appropriate use of student email:

   All use of email will be consistent with other college policies, including the "GCC Acceptable Use Policy," which can be found at:

http://www.glendale.edu/index.aspx?page=1782

Deleted: http://www.glendale.edu/GCCDesktopPolicy.htm ¶

2. Assignment of student email

   Official college email accounts will be created automatically for all enrolled students at the time of registration. Official email addresses will be directory information unless the students request otherwise.

   - Email addresses will be configured using the first letter of the first name, the first 6 letters of the last name and the last 3 digits of the student ID.

Deleted: as

Deleted: :

Deleted: <#>First Name.Last Name¶

Deleted: <#>Duplicates:¶ <#>First Name.Middle Initial.Last Name¶

Deleted: <#>Third Duplicate:¶ <#>First Initial.Last Name¶

Deleted: *Or: First Name.Last Name + (Year Enrolled or Other Number)¶

   - If a student has not been enrolled for three consecutive primary terms, the user account will be deleted.

Deleted: semesters

   Specific student email directions are online at: mygcc.glendale.edu

3. Expectations of student use of email

   Students are expected to read and respond as appropriate to their GCC official email on a frequent and consistent basis. The college recommends checking email daily since certain communication may become critical.

4. College use of email

   Email is a mechanism for official communication within Glendale Community College. The college expects that students will open and read such communications in a timely fashion. Official email communications are intended only to meet the academic and administrative needs of the campus community.

5. Faculty Use of email

   Faculty will determine how electronic forms of communication (e.g., email) will be used in their classes and will specify their requirements in the course syllabus. This official student email policy will ensure that all students are able to comply with email-based course requirements specified by faculty. Faculty can therefore make the assumption that students' official email accounts are being accessed and they can use email for their classes accordingly.

6. Redirecting of student email

   The GCC assigned email address will be the address used by GCC staff/faculty to communicate with students. Students who redirect (auto forward) messages sent to their official GCC student email address to another address (such as AOL, Yahoo, Hotmail, etc.), do so at their own risk. Having email lost as a result of redirection does not absolve the student from responsibilities associated with communication sent to his/her official GCC email address. The college is not responsible for the handling of email by outside vendors.

7. Authentication for confidential information.

   It is a violation of college policies, including the Student Code of Conduct, for any user of official email addresses to impersonate a college office, faculty/staff member, or student. To minimize this risk, some confidential information may be made available only through Student Self Service Web Access, which is password protected. In these cases, students will receive email correspondence directing them to Student Self Service Web Access (MyGCC), where they can access the confidential information only by supplying their student ID and PIN. The confidential information will not be available in the email message.

8. Privacy

   Email users should exercise extreme caution in using email to communicate confidential or sensitive matters and should not assume that email is private and confidential. It is especially important that users be careful to send messages

only to the intended recipient(s). Particular care should be taken when using the "reply" command during email correspondence, because many mailing lists are configured to deliver replies to the entire list, not just the author of a given message.

- Confidentiality of student records is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA). All use of email, including use for sensitive or confidential information will be consistent with FERPA.

9. Name Changes for the student email policy

   Electronic mail is considered an official method for communication to Glendale Community College students.

   Name changes will affect your student email address. If you request a name change, a new email address will be created at the end of the semester.

   Continue to check your existing email account until you receive a letter notifying you of your new email address.

POLICY REVIEW

The Campuswide Computer Coordinating Committee will review this policy as needed.

To: 4C Members

From: Arnel Pascua, Chair

Date: January 21, 2010

Subject: Proposed Changes to Student Email Policy

I found out from reviewing the Campus Exec meeting minutes that the Student Email Policy was approved, but Campus Exec requested a minor change as stated in the minutes (excerpt shown below) of their meeting on 12/9/2008.

CONSENT CALENDAR

The Consent Calendar was approved as amended: • *Page 2 – Campus Wide Computer Coordinating – October 23, 2008* ◆Dr. Queen requested a copy of the "Student Email Policy." ◆The word "Policy" will be changed to "Procedures." Mr. Serot will ask staff to make this change. • *Page 4 – Foundational Skills – October 6, 2008* There was a brief discussion on the motion approving 80% released time for the coordinator of the Basic Skills Initiative Grant for the term of 2 ½ years. It was was determined that the position could be advertised, but that the position is ultimately dependent upon funding, and therefore could be revisited in the future.	• *It was moved (Dr. Queen) and seconded (Dr. Perez) that the Consent Calendar prepared for the December 9, 2008 Executive Committee Meeting be approved with one amendment and one request. The motion passed unanimously.*

Second, the PeopleSoft steering committee approved at its November 5, 2009 meeting a student email account naming convention that is different from what is stated in the policy. Third, the link to the GCC Acceptable Use Policy has changed due to the launching of the new web site. Fourth, the word "semesters" was changed to "primary terms" for clarity.

Therefore, I propose these minor changes and attached a copy of the policy for your reference.