Grayson College
Computer Use Policy

Adopted March 21, 2000

Introduction

Grayson College provides each of its students, faculty and staff with one or more computer accounts that permit use of the college's computer resources. Use of these resources is a privilege, not a right. When using these resources, individuals agree to abide by the applicable policies of the College, as well as federal, state and local laws. The College reserves the right at any time to limit, restrict or deny access to its computer resources, as well as to take disciplinary and/or legal action against anyone in violation of these policies and/or laws.

Applicable Policies, Procedure and Law

The policies and procedures which apply to users of College computer resources include, but are not limited to, this policy, as well as College policies against harassment, plagiarism, and unethical conduct and any procedures which govern computer usage at a particular facility on campus. Laws which apply to users of College computer resources include, but are not limited to, federal, state and local laws pertaining to theft, copyright infringement, insertion of viruses into computer systems, and other computer related crimes. This policy applies to all College computer resources, whether administered centrally or within a department, single or multi-user, mainframe or network server, etc. Computer resources include hardware, software, communications networks, electronic storage media, and manuals and other documentation. Data includes all files, regardless of size or storage media, including e-mail messages, system logs, and software (commercial or locally developed).

Principles

The following principles address the general philosophy of Grayson College on computer use and security. These principles apply to and are binding on all users of College computer resources:

1. Authorized Use: Grayson College provides computer resources for the purpose of accomplishing tasks related to the College's mission.

   It should be noted that the use of some of the computers, networks, and software located on the College campus may be dedicated to specific aspects of college missions or purposes that limit their use or access.

   Students, including incoming students who have paid their fees, shall be allowed to use the College's computer resources for school-related and incidental purposes, subject to this policy and other applicable College policies; state and federal law; and as long as personal use does not result in any additional costs to the College. Graduating students and students who leave the College for any reason will have their computer access rights terminated, except that, with the permission of the appropriate system administrator(s), continuing students enrolled for the coming fall semester may retain their computer rights during the summer.

   An employee of the College shall be allowed to use computer resources in accordance with this and other applicable College policies. Incidental personal use of computer resources by employees is permitted, subject to review and reasonable restrictions by the employee's supervisor; adherence to applicable College policies and state and federal law; and as long as such usage does not interfere with the employee's accomplishment of his or her job duties and does not result in any additional costs to the College. When an employee terminates employment, his or her access to the College's computer resources will be terminated immediately.

2. Freedom of Expression: Censorship is not compatible with the goals of higher education. Grayson College does reserve the right, however, to place reasonable time, place and manner restrictions on freedom of expression on its computer systems.

3. Privacy: Users of the College's computer systems should be aware that computer use may be subject to review or disclosure in accordance with the Texas Public Information Act and other laws; administrative review of computer use for security purposes or in regard to a policy or legal compliance concern; computer system maintenance; audits and as otherwise required to protect the reasonable interests of the College and other users of the computer system. Anyone using the College's computer systems expressly consents to monitoring on the part of the College for these purposes and is advised that if such monitoring reveals possible evidence of criminal activity, College administration may provide that evidence to law enforcement officials. Further, all users should understand that the College is unable to guarantee the protection of electronic files, data or e-mails from unauthorized or inappropriate access.

4. Intellectual Property: All members of the College community should be aware that intellectual property laws extend to the electronic environment. Users should assume that works communicated through the computer network are subject to copyright laws, unless specifically stated otherwise.

5. Valuable assets: Computer resources and data are considered valuable assets of the College. Further, computer software purchased or leased by the College is the property of the College or the company from whom it is leased. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of any of these assets may constitute a computer-related crime, punishable under Texas statutes and federal laws. College computer resources may not be transported without appropriate authorization.

Misuse of Computing Resources

The following actions constitute misuse of the College's computer resources and are strictly prohibited for all Users:

1. Criminal and illegal acts. College computer resources are not to be used in support of or for illegal activities. Any such use will be reported and dealt with by the appropriate College authorities and/or law enforcement agencies. Criminal and illegal use may involve, but is not limited to, unauthorized access, intentional corruption or misuse of computer resources, theft, obscenity, and child pornography.
2. Failure to comply with laws, policies, procedures, license agreements, and contracts that pertain to and limit the use of the College's computer resources.
3. Abuse of computer resources including, but not limited to, any act which endangers or damages specific computer software, hardware, program, network or the system as a whole, whether located on campus or elsewhere on the global Internet; creating or purposely allowing a computer malfunction or interruption of operation; injection of a computer virus on to the computer system; sending a message with the intent to disrupt College operations or the operations of outside entities; print outs that tie up computer resources for an unreasonable time period; and failure to adhere to time limitations which apply at particular computer facilities on campus.
4. Use of College computer resources for personal financial gain or a personal commercial purpose.
5. Failure to protect a password or account from unauthorized use.
6. Permitting someone to use another's computer account, or using someone else's computer account.
7. Unauthorized use, access or reading of any electronic file, program, network, or the system.
8. Unauthorized use, access, duplication, disclosure, alteration, damage, or destruction of data contained on any electronic file, program, network, or College hardware or software.

9. Unauthorized duplication of commercial software. All commercial software is covered by a copyright of some form. Duplication of software covered by such copyrights is a violation of the copyright law and this policy.
10. Attempting to circumvent, assisting someone else or requesting that someone else circumvent any security measure or administrative access control that pertains to College computer resources.
11. Use of the College computer system in a manner that violates other College policies such as racial, ethnic, religious, sexual or other forms of harassment.
12. Use of the College's computer system for the transmission of commercial or personal advertisements, solicitations, promotions, or political material except as may be approved by the Office of the Vice President of Information Technology.

Email as Official Communication

Grayson College faculty and staff are provided with e-mail accounts for the purpose of conducting official college business related to instructional, academic and/or administrative activities to accomplish tasks consistent with the college's mission. Because email is an effective way to disseminate information of importance, relevance and interest, and because it is an important tool to meet the academic and administrative needs of the college community, it shall be college policy that electronic mail (email) be an official communication mechanism with faculty and staff, and that all faculty and staff are required to maintain a grayson.edu email address. This is the only email address that will be used for official communication with faculty and staff regarding all academic and administrative matters.

This policy does not preclude the use of conventional methods of communication.

1. Acquiring an email account: Official college email accounts are available to all current faculty and staff. These accounts must be activated before the college can send correspondence using official email addresses. Faculty and staff may activate their email accounts by contacting the Computer Services department. Official email addresses will be maintained in college information system and will be included in the college's directory.

2. Redirecting/forwarding of email: Grayson College recommends against forwarding Grayson College email to an external email account, but if Grayson email is forwarded to an external account, for archiving purposes, official GC email sent from that external account must be sent as the Grayson.edu user. Official GC email that originates from an external account won't be archived if the email isn't sent as the Grayson.edu user. If faculty or staff wish to have email redirected/forwarded from their official grayson.edu address to another email address (e.g., @aol.com, @Yahoo.com, etc.), they may do so at their own risk. The college shall not be responsible for the handling of email by outside vendors. Having email redirected does not absolve faculty or staff from the responsibilities associated with official communication sent to their grayson.edu account.

3. Expectations about use of email: Senders of e-mails should identify themselves as representatives of the college by including their title or function at the end of the message. It is inappropriate to include statements or quotations in the body or signature portion of the message that do not directly advance the administrative or academic purpose of the message. Email users should avoid using language that could be offensive to others, or create an atmosphere of discomfort. Content and signature information of electronic messages should be focused on official college business.

4. Access to Email: Supervisors must provide computer access to employees whose positions do not provide them with regular access to a computer, as well as a reasonable amount of time to use the computer provided for the purpose of checking their email for college business.

5. Confidentiality: Users should exercise extreme caution in using email to communicate confidential or sensitive matters (e.g. individual personnel actions), and should not assume that email is private and confidential. It is especially important that users are careful to send messages only to the intended

recipient(s). Particular care should be taken when using the "reply" and “reply all” command during email correspondence.

6. GC People Email: The GC People email system is an important tool for communicating information that a large part of the campus community needs to know. The system should only be accessed when a minimum of seventy-five percent of the campus community needs to be made aware of the information. First and foremost, the system is crucial for communicating about emergencies. Therefore, it is essential that the system not be overly used whereby members of our campus feel “spammed” and begin to ignore its messages. Announcements are limited to information about emergencies and safety; presidential communications; major campus events; critical alerts related to human resources, facilities and technology; and key internal processes, procedures and deadlines that affect the majority of the campus or a specific targeted group.

   Campus members wishing to send a GC People message that does not meet the specified criteria—information about emergencies and safety; presidential communications; major campus events; critical alerts related to human resources, facilities and technology; and key internal processes, procedures and deadlines that affect the majority of the campus or a specific targeted group—must submit their requests in writing to their Vice President for approval.

Responsibilities of Grayson College Computer Users

1. A user shall use the College computer resources responsibly, always respecting the rights of other computer users by not displaying materials that are offensive to others.
2. A user is responsible for any usage of his or her computer account. Users should maintain the secrecy of their password(s).
3. A user must report any misuse of computer resources or violations of this Policy to their department head or to the Office of the Vice President of Information Technology.
4. A user must comply with all reasonable requests and instructions from the computer system operator/administrator.
5. When communicating with others via the College computer system, a user's communications should reflect high ethical standards, mutual respect and civility.
6. Users are responsible for obtaining and adhering to relevant network acceptable use policies.

Responsibilities of Deans, Department Heads, and Supervisors

1. Ensure that employees within a department receive training to comply with this policy.
2. Promptly inform appropriate computer system administrators when employees have been terminated so that the terminated employee's access to College computer resources may be disabled.
3. Promptly report ongoing or serious problems regarding computer use to the Office of the Vice President of Information Technology.

Auditor Access of College Computing Resources

Authorized auditors will be provided access to college computer resources and data files as needed.

Information Security

The objective of the Grayson College Sensitive Information Policy is to advise and govern faculty, staff, and students on the storage and release of sensitive information at Grayson College.

Definitions

For the purposes of this policy, sensitive information is an individual's name, address, or telephone number combined with any of the following:

Social security number or taxpayer ID number.
Financial account, credit or debit card number.
Financial/salary data.
Driver's license number.
Date of birth.
Medical or health information protected under state or federal law (e.g. HIPAA).
Student data protected under state or federal law (e.g. FERPA).
Access codes, security codes or passwords that would permit access to sensitive information.

In addition, the security of other types of sensitive or confidential information is provided for in this policy. This includes, but is not limited to, information relating to any of the following:

Current or future fundraising campaign strategies.
Donor information such as wealth, asset holdings, and giving history, internal and external to Grayson College.
Planning and construction of facilities.
Information regarding Grayson's current or projected financial matters, including its schools and programs.
Vendor proprietary information (e.g. information from a third-party held confidential by agreement).
Information explicitly marked as confidential (e.g. documents prepared for the Board of Trustees).

Storage and Access of Sensitive Information

Remote Access

All remote access to sensitive information contained in applications and servers must be managed and secured exclusively by Information Technology. Information Technology provides remote access to applications and servers for this purpose. In all cases, data security can more easily be maintained and verified within the confines of Grayson College, than on personally owned laptops and computers. Transporting unencrypted sensitive information on portable devices, such as laptops, CD media, or USB keys, which are subject to loss or theft, is not allowed.

Physical Access

Often times, gaining physical access to or observing the use of a computer can result in impermissible disclosure of sensitive information. Grayson College requires steps to reduce the possibility of accidental disclosure in this manner including:

Using an automatically activated screensaver password to secure the computer when it is unattended.
Positioning monitors to prevent inadvertent disclosure of sensitive information on screens, or if repositioning is not possible, using physical screen guards.
Securing computer and portable media physically from theft or tampering by locking them within a secure area or securing them with a cable lock or audible alarm.
Implementing tools that aid in the identification of persons who unlawfully gain access to sensitive information to facilitate disciplinary action and/or prosecution by law enforcement agencies.
Storing documents and data in a coded or encrypted form.

Virus Protection

Virus and malware constitute a significant threat to sensitive information and may allow unwanted disclosure. All Grayson College computers are equipped with virus and malware protection. Faculty and staff with Administrative Rights to Grayson College computers shall not alter or disable this protection. All computers, including those personally owned and attached to the campus network or used for the processing or storage of sensitive information, must have virus protection installed and up-to-date. Additionally, all computers must have their operating system and software security patches up-to-date.

Permissions and Passwords

Remote access to applications and systems is granted by authentication and authorization systems managed by Information Technology. In most cases, access is allowed via username and password. Faculty, staff and students must take precautions to safeguard usernames and passwords including:

- Not writing usernames and passwords down or keeping them where others could gain access.
- Never sharing or divulging to anyone usernames or passwords, including others at Grayson College.
- Choosing strong passwords, including both letters (upper and lower case) and numbers (e.g. MyGrayson1965).
- Not entering passwords on computers that have potential to be compromised, such as public computers in Internet cafés or airports.
- Refraining from saving or caching passwords in browsers or other applications.

Encryption

Any sensitive information downloaded from secure applications or servers to a non-college owned computer, laptop, or portable device or media shall not be stored unencrypted beyond the session of computer use in which it was downloaded. Such sensitive information must be either encrypted or deleted immediately after use.

Retention and Destruction of Sensitive Information

In some cases, the retention of data may be mandated by government and/or other regulations. In such cases, retention of data shall comply with these rules. Otherwise, copies of sensitive information that are made for a specific purpose must be deleted after that purpose has been fulfilled. In the case of paper or other disposable media, such as CDs, floppies, or magnetic tape, destruction should be complete and permanent. For assistance or advice, please contact the Help Desk.

If you have access to or copies of sensitive information in your possession or under your control, you are responsible for surrendering that information upon termination of your employment. Your manager, Dean, Vice President, or a member of Human Resources will work with you to assist you in this critical task prior to your last day of work. No employee - faculty or staff - should delete information at the conclusion of employment without consulting his/her supervisor.

Note: If your position gives you access to sensitive information as defined in this policy, your Grayson College email, computer, and network access shall be terminated immediately upon the conclusion of your employment.

Policy Compliance and Incident Response

All persons with access to sensitive information at Grayson College are responsible for compliance with this policy. Violations of this policy are serious and may result in disciplinary action up to and including termination of employment. Any disclosures of sensitive information that are not for Grayson College business purposes shall be reported expeditiously to the Office of the Vice President of Information Technology.

Such report shall include:

- The type and scope of information disclosed (who, what, when).
- Circumstances under which the disclosure occurred (where, how).

Contractors with whom the College shares sensitive information or who have incidental access to sensitive information within the scope of their work shall either sign an agreement acknowledging this policy and assuring to keep such information protected and confidential, or submit a copy of their company policy on confidentiality and protection of sensitive information for review and approval by the Vice President of Information Technology.

Potential Liability for Failure to Adhere to this Policy

It is important to note that failure to adhere to this Policy may lead to the cancellation of a user's computer access, suspension, dismissal, or other disciplinary action by the College, as well as referral to legal and law enforcement agencies.

The following are some laws that pertain to computer usage:

Texas Administrative Code, 201.13(b): Information Security Standards

State of Texas law that sets forth the requirements state entities must follow regarding computer security.

Texas Penal Code, Chapter 33: Computer Crimes

State of Texas law specifically pertaining to computer crimes. Among other requirements, unauthorized use of College computers or unauthorized access to stored data, or dissemination of passwords or other confidential information to gain access to the College's computer system or data is in violation of criminal law.

Texas Penal Code, Chapter 37: Tampering with Governmental Record

Any alteration, destruction, or false entry of data that impairs the validity, legibility or availability of any record maintained by the College is a violation of criminal law.

United States Penal Code, Title 18, Section 1030: Fraud and related activity in connection with computers

Federal law specifically pertaining to computer crimes. Among other requirements, prohibits unauthorized and fraudulent access.

Federal Copyright Law

Recognizes that all intellectual works are automatically covered by copyright. The owner of a copyright holds the exclusive right to reproduce and distribute the work.

Computer Fraud and Abuse Act of 1986

Makes it a crime to access a computer to obtain restricted information without authorization; to alter, damage, or destroy information on a government computer; and to traffic in passwords or similar information used to gain unauthorized access to a government computer.

Electronic Communications Privacy Act of 1986

Prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal.

Computer Software Rental Amendments Act of 1990

Deals with the unauthorized rental, lease, or lending of copyrighted software.