

Grayson County College

Computer Use Policy

Adopted March 21, 2000

Introduction

Grayson County 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 County College on computer use and security. These principles apply to and are binding on all users of College computer resources:

Authorized Use: Grayson County 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.

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

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.

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.

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 Dean of Information Technology.

Responsibilities of 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 Dean 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 Dean of Information Technology.

Auditor Access of College Computing Resources

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

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.