



[IT Home Page](#) | [Information](#) | [About IT](#) | [Support](#) | [PeopleSoft](#)

## Policy and Procedures

### **About IT**

[Vision, Mission & Guiding Principles](#)

[2005-2006 Proposed Projects](#)

[IT Staff](#)

[Policies & Procedures](#)

[IT in Action \(Photos\)](#)

Given the rapid pace of technological change, decentralization of computing and the proliferation of computers, network and users of varying capabilities, it is essential that these systems be protected from misuse and unauthorized access. The Information Technology and Telecommunications Policy is intended to represent all computing and telecommunications facilities and refers to all hardware, data, software, networks and facilities associated with information resources at Lee College.

Telecommunications equipment, including computer systems, e-mail, voice mail, networks and associated facilities, provided by Lee College are owned by the college and are only to be used to support the instruction and administrative functions of Lee College. If faculty, staff or students bring personally-owned equipment into the Lee College environment, they will be required to adhere to existing campus policies and standards as use of their equipment may compromise data and network security and affect the work of others.

Lee College reserves the right to limit, restrict or extend computing and telecommunication privileges and access to its information resources. Information Technology and Telecommunications resources are not to be used for commercial purposes or for non-college related activities without written authorization from the Technology Advisory Committee (TAC).

All members of the Lee College District who use the college's Information Technology and Telecommunications equipment and information resources must act responsibly. All uses of college-owned or college-leased computing and telecommunications equipment must respect the rights of other users, respect the integrity of the physical facilities and controls and respect all pertinent license and contractual agreements.

### **Unacceptable Use**

Unacceptable use includes but is not limited to the following:

- Misrepresenting your identity or affiliation through the use of computers and telecommunications equipment.
- Sending harassing, intimidating, abusive or offensive material to or about others.
- Intercepting, disrupting or altering electronic communications packets.
- Causing congestion on the network or voice mail equipment by such things as the propagation of "chain letters", "broadcasting" inappropriate messages to lists or individuals or excessive use of the shared data store on the e-mail post office.

### **Enforcement**

Failure to adhere to the Information Technology and Telecommunications Policy could result in suspension of usage privileges.

**Also see:**

[Internet Acceptable Use Policy](#)

[Contractor Support Procedures](#)

[E-Mail Guidelines](#)

[Library Acceptable Use Policy](#)

[Using Software](#)

[Virtual Private Network Policy](#) (*Adobe .pdf*)



## Office of Information Technology

[IT Home Page](#) | [Information](#) | [About IT](#) | [Support](#) | [PeopleSoft](#)

### Policy and Procedures

## Information Resources Acceptable Use Policy

#### About IT

[Vision, Mission & Guiding Principles](#)

[2005-2006 Proposed Projects](#)

[IT Staff](#)

[Policies & Procedures](#)

[IT in Action \(Photos\)](#)

The primary mission of Lee College is to provide quality instruction for its students. Through a variety of programs and services, Lee College prepares students for success in higher education or employment. Lee College also provides a broad-based program of extension courses, adult education, community education and services. It is the policy of Lee College District to apply the highest ethical standards to all members of the college community including the Board of Regents, administration, staff and faculty in achieving its mission and in managing its resources efficiently and effectively to reach its goals and objectives.

Faculty, staff and student (hereinafter users) are expected to promote efficient use of network resources, consistent with the instructional, research, public service and administrative goals of the College. Refrain from engaging in any use that would interfere with work or disrupt the intended use of network resources. It is not responsible to use disproportionate amounts of electronic resources. Examples of disproportionate uses generally include activities such as serving MP3 music, streaming media at high bit rates or serving a multi-user game or host.

Lee College relies heavily on networked computers and the data contained within those systems to achieve its missions. Users are notified that electronic information is not private and remains the property of Lee College. This Acceptable Use Policy is to protect these resources in accordance with the State of Texas laws, Federal laws and [Lee College Board Policy](#). All users (administrators, faculty, students and visitors) granted access to Lee College Information Resources must follow the acceptable use policy below.

#### Acceptable Use of College Information Resources

- Lee College Information Resources are provided for faculty, staff and students to use in the pursuit of the teaching, educational and service mission of the college.
- Lee College email is to be used to enhance and facilitate teaching, learning, scholarly research, support academic experiences and to facilitate the effective business and administrative processes of the College.
- Acceptable use of Lee College network resources should be used for electronic dissemination of information, including the establishment of web sites, publishing web documents, and creating web applications as well as the distribution of bulletins, memoranda, newsletters, reports, and committee communications; instructional use specifically to enhance communications between students and instructors, facilitation of distance learning and support of Lee College scholarly activities; business and service activities of faculty and staff and uses as are consistent with the traditional academic freedom accorded to faculty members.
- Administrative activities that are part of the support infrastructure needed for instruction, scholarship, and institutional management of the member institutions.
- Research, scholarship, or instructional applications engaged in by students, faculty and staff.
- Communication and exchange for professional development, to maintain currency, or to debate issues in a field or sub-field of knowledge.
- Applying for or administering grants or contracts for research or instruction.
- Fundraising, solicitation, or public relations activities related specifically to the mission, strategic plan, and development of the institution.
- Announcements of new products or services used in research or in instruction.
- Administrative, academic, and research-related discussion groups on a wide variety of topics.
- Users are expected to be knowledgeable of, and to perform their duties in compliance

	<p>with, federal, state, and local laws and college policies, including the provisions of the Family Educational Rights and Privacy Act designed to protect the confidentiality of data and the privacy of individuals.</p> <ul style="list-style-type: none"> <li>• Users are expected to access information that is needed in the context of the performance of their normal duties and to exercise good judgment in the use of such information. In particular, confidential or demographic data, which pertains to students, employees, or college operations, must be used in a manner that protects rights of privacy and limits personal and institutional liability. In general, employees are expected to avoid situations in which they either provide or interpret to others information which is outside the scope of their expertise or job responsibilities.</li> </ul>
Data Protection Copyright	<ul style="list-style-type: none"> <li>• All confidential information transmitted over external networks or saved on system servers must be encrypted, must not be sent or forwarded through non-Lee College email accounts (like Hotmail, Yahoo mail, AOL mail, etc.), and must not be knowingly transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols and security techniques are utilized.</li> <li>• Users of Information systems must not attempt to access data or programs contained on systems for which they do not have authorization by the system owner.</li> <li>• Staff must not copy or reproduce any licensed software except as expressly permitted by the software license, use unauthorized copies on college-owned computers or use software known to cause problems on system computers (approval from the Office of Information Technology).</li> <li>• Any critical Lee College data stored on Lee College workstations must be backed up in their home directory or external media in the event of a disaster or loss of information.</li> <li>• Users may not use the Internet for activity prohibited by federal law. Some material on the Internet may be protected by federal copyright laws (see generally <a href="#">Title 17, United State Code</a>).</li> <li>• Unauthorized reproduction or distribution of copyrighted materials is illegal, except as permitted by the principles of "fair use." Generally, fair use of copyright materials is limited to copies made for personal use, private study, scholarship, or research. If the use of copyrighted material does not fall within fair use, permission from the copyright holder to use the material must be obtained before any such use. If in doubt about whether or not your use may infringe on material protected by a copyright, ask the copyright owner for permission to use the protected material.</li> <li>• Exchanging digital copies of music files, often in the "MP3" format has become popular. Posting on the network, or in any other way (streaming server) exchanging copies of songs from commercial music CD's is <b>illegal</b>.</li> <li>• Students should be aware that certain aspects of their privacy relating to academic records are governed by the Family Educational Rights and Privacy Act (FERPA). Details of that law are available in the Lee College Catalog. Refer to the following link: <a href="http://www.lee.edu/catalog.asp">http://www.lee.edu/catalog.asp</a>.</li> </ul>
Virus Protection	<ul style="list-style-type: none"> <li>• All computers connecting to the Lee College network must run current site-licensed virus prevention software.</li> <li>• Centrally provided virus protection software must be ran on all computers connected to LEENet.</li> <li>• With the exception of installation of software, or other special circumstance or procedure that requires the temporary disabling of virus prevention software, such software must not be disabled or bypassed.</li> <li>• If deemed necessary to prevent viral propagation to other networked devices or detrimental effects to the network, computers infected with viruses or other forms of malicious code shall be disconnected from the network until the infection has been removed.</li> <li>• Users must perform regular backups. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.</li> <li>• Periodically check your computer and be certain that the virus protection software is running correctly and that system security patches are applied. OIT regularly remotely downloads up-to-date security patches (DATs) to computers that are able to accept the update.</li> </ul>

<p><b>E-mail</b></p>	<ul style="list-style-type: none"> <li>• The following email activities are prohibited by policy:             <ul style="list-style-type: none"> <li>- Using email for purposes of political lobbying or campaigning.</li> <li>- Posing as anyone other than oneself when sending email.</li> <li>- Reading another User's email unless authorized to do so by the owner of the email</li> <li>- Using email software that poses high security risks to Lee College Information Resources.</li> <li>- Sending unsolicited messages, except as required to conduct Lee College business.</li> <li>- Sending excessively large messages or attachments unless for office College business.</li> <li>- Sending or forwarding email that is likely to contain computer viruses.</li> </ul> </li> <li>• Email messages may not include any user's identification number (e.g., social security number), should include only unique identifying information that is pertinent to the message being conveyed and should not reference any student's academic record or confidential employee information.</li> <li>• Altering electronic communications to hide one's identity or to impersonate another individual is considered misrepresentation and/or forgery and is prohibited under this policy. All email, news posts, chat sessions, or any other form of electronic communication must contain the sender's real name and/or email address.</li> <li>• Initiating or forwarding "chain letters" or email is prohibited on the college email systems and the Internet as a whole. Chain email can be identified by phrases such as "please pass this on to your friends" or similar inducements that encourage you to forward the message.</li> <li>• User should avoid opening messages or attachments received from unknown senders or responding to instant messages or other peer to peer technologies from strangers. Messages and attachments can carry viruses. IM (instance messaging and peer to peer technologies) are often used by intruders with malicious intent. Non-business related Instance Messaging should be avoided.</li> <li>• Address messages to recipients who "need to know." Messages sent unnecessarily to a long list of recipient's lowers system performance.</li> <li>• You may not be paid, or otherwise profit, from the use of any College-provided computing resource or from any output produced using it. You may not promote any commercial activity using College resources. Use of email for profit-making activities (sales or distribution of commercial products or services for profit, etc.) including product advertisement and mass mailings or use by for-profit companies is unacceptable unless otherwise authorized by the President of Lee College.</li> <li>• The use of email or any college system for harassment or criminal activity may result in criminal penalties, including fines and imprisonment.</li> </ul>
<p><b>Use of Information Resources</b></p>	<ul style="list-style-type: none"> <li>• Storage of any non-work related email messages; voice messages, files and documents within the Lee College email system must be nominal (less than 5% of a User's allocated mailbox space) unless stored on the hard drive or external media.</li> <li>• Use of personal software and hardware on College computers is prohibited without authorization by the Director of Information Technology. Software is subject to licensing and all license provisions (including copyright, use, duplication, simultaneous use, etc.) must be honored.</li> <li>• Non-work related files may not be stored on network file servers.</li> <li>• Any files, messages or documents residing on Lee College computers may be subject to public information requests and may be accessed in accordance with this policy.</li> <li>• Commercial network resources and software that are licensed by Lee College for internal use only may not be used outside the College network.</li> </ul>
<p><b>Internet Use</b></p>	<ul style="list-style-type: none"> <li>• Users shall not use the Internet connection to perform any act that may be construed as illegal or unethical, including attempting to gain unauthorized access to the network.</li> <li>• To insure the best overall network performance, network traffic will be monitored. OIT will take appropriate action if any computer causes traffic problems that interfere with the business of the Lee College. If, in the course of monitoring network traffic, information which may have adverse legal implications for Lee College is discovered, it will be reported.</li> <li>• Both personal and commercial advertising must not be posted on Lee College web sites.</li> <li>• Users shall not engage in activities that relate to material involving the sexual exploitation of minors as defined by <a href="#">Federal Code Title 18, Part I, Chapter 110, Sexual Exploitation and other abuse of children</a> or other criminal acts.</li> </ul>

Portable and Remote Computing	<ul style="list-style-type: none"> <li>• All computers and/or portable-computing devices using Lee College Information Resources must be password protected and be changed when prompted according to password authentication policy timeline of every 90 days or if the password is suspected of being compromised.</li> <li>• Employees accessing the Lee College network from a remote computer must adhere to all policies that apply to use from within Lee College facilities, must conform to the OIT minimum standards for portable computing, and are subject to the same rules and security related requirements that apply to college owned computers.</li> <li>• All hardware that connects to the Lee College network must be installed by certified Office of Information Technology technicians and network administrators.</li> </ul>
Passwords	<ul style="list-style-type: none"> <li>• Lee College account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes must not be shared and are non-transferable. Owners are responsible for all usage of their assigned accounts, log-ons and passwords.</li> <li>• Digital certificate passwords used for digital signatures must never be divulged to anyone.</li> <li>• Users must not circumvent password entry through use of auto logon, application "remember password" features, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Lee College Information Technology Director. Any exception situation must include a procedure to change the passwords and must adhere to security policies for password construction.</li> <li>• Users may not attempt to evade, disable, or "crack" passwords or other security provisions. These activities threaten the work of others and are grounds for immediate disciplinary action. Unauthorized copying of files or passwords belonging to others or to the College may constitute plagiarism or theft. Modifying files without authorization (including altering information, introducing viruses or Trojan horses, or damaging files) is unethical, may be illegal and can lead to disciplinary action.</li> <li>• Users must establish appropriate passwords, change them as required and never share them with others.</li> </ul>
Telephone Long Distance Access Code	<ul style="list-style-type: none"> <li>• Users shall not tap phone/data lines or accessing files by circumventing security restrictions.</li> <li>• Each individual who is authorized by a division/department to place long distance calls for Lee College business will be issued an individual authorization code which can be used to place calls from Lee College phones.</li> <li>• Telephone services and wiring may not be modified or extended beyond the area of their intended use.</li> <li>• Unauthorized use of an individual's telephone extension number or voice mailbox and any attempt to gain access to a voice mailbox other than your own is prohibited. Voice mailbox passwords should never be exchanged.</li> <li>• Users are not permitted to accept collect calls, arrange for third party billing to their campus telephone extension or place operator assisted calls that result in a charge to the college. Any campus telephone extension determined to be accepting or making such calls will be subject to a fine plus the cost of the call(s).</li> <li>• Attempting to place a billable call from any college telephone without paying for the service may constitute theft. Telecommunications will levy a fine for investigation plus the cost of the telephone call(s).</li> </ul>
CyberSecurity	<ul style="list-style-type: none"> <li>• Security programs or utilities that reveal or exploit weaknesses in the security of a system or that reveal data by circumventing established authorization procedures and systems should not be downloaded and/or used, except as authorized by the OIT. For example, password cracking programs, packet sniffers, wireless hubs or port scanners on Lee College Information Resources shall not be used. Users must report any identified weaknesses in Lee College computer security and any incidents of possible misuse or violation of this agreement to the Director of Lee College Information Technology Office.</li> <li>• Due to the open and decentralized design of the Internet and networked computer systems, Lee College cannot protect individuals against the receipt of material that may be offensive to them. Likewise, individuals who use e-mail or those who make information about themselves public on the Internet should know that Lee College cannot protect them from invasions of privacy. It is recommended that users utilize the network only for business related activities of the college.</li> <li>• Do not download and/or use tools that are normally used to assess security or to attack computer systems or networks (i.e. password "crackers", vulnerability scanners, network sniffers, etc.) unless you have been specifically authorized to do so by I.T.</li> <li>• Each user is responsible for the security of any system he/she connects to the network. A system seen to be attacking other systems, e.g. having fallen victim to viruses/worms, will be taken off the network, generally without notice, until it has been made secure.</li> <li>• Users may not operate network services from their computers (BBS, Chat, DHCP, DNS, anonymous FTP, IRC, NNTP, POP2/POP3, SMTP, etc.). Users who have a bona fide academic need to operate such services must obtain written authorization from the OIT</li> </ul>

	<p>Director prior to activating any such service.</p> <ul style="list-style-type: none"> <li>• Users may not conduct port scans on the campus network, or of outside networks from the campus network, may not operate Ethernet cards in promiscuous mode, or use any IP address on the campus network other than those assigned by the College.</li> <li>• Lee College network services and wiring may not be modified or extended. This applies to network wiring, hardware, and in-room jacks. Use of Ethernet switches, network hubs, or wireless networking technology on the campus network is expressly prohibited and can impose unnecessary security vulnerability on the network.</li> <li>• A computer owned personally by a student, faculty member or staff member is subject to College policy while it connects to the College network directly or through a dialup connection. An individual may not grant access privileges to other individuals on a computer in violation of the general eligibility policy below, even if that computer is personally owned. If a computer is connected to the College network, access from that computer to the rest of the campus network can only be made available to individuals otherwise authorized to use the campus network. This includes email, Web services, file transfer, Internet Relay Chat (IRC), telnet, and any other network traffic.</li> <li>• The installation of any type of device that allows the sharing of a single IP address by multiple devices compromises the operation of the network and must not occur. This includes proxy servers, personal routers or any other type of network equipment. It is expected that each end-user device will be configured with a single registered IP address from the campus Network Operations Center.</li> <li>• The College is bound by its contractual and license agreements respecting certain third party resources; you are expected to comply with all such agreements when using such resources.</li> </ul>
<p><b>Your Rights and Responsibilities</b></p>	<ul style="list-style-type: none"> <li>• As a member of the Lee College community, the college provides you with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet. You have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether you are a college employee or student), and of protection from abuse and intrusion by others sharing these resources. You can expect your right to access information and to express your opinion to be protected as it is for paper and other forms of non-electronic communication.</li> <li>• In turn, you are responsible for knowing the regulations and policies of the College that apply to appropriate use of the College's technologies and resources. You are responsible for exercising good judgment in the use of the College's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.</li> <li>• As a representative of the Lee College community, you are expected to respect the College good name in your electronic dealings with those outside the College.</li> </ul>
<p><b>Violations of AUP</b></p>	<ul style="list-style-type: none"> <li>• Users are expected to notify the Office of Information Technology, classroom instructor, lab supervisor, or other responsible party, as appropriate, of intentional or unintentional breaches in access and data security of which they become aware. In addition, employees who are aware of serious violations of acceptable use or related policies and procedures (including malicious tampering, virus infection, spyware, phishing or "hacking") are required to report such activity to their immediate supervisors.</li> <li>• Policies and guidelines are established to maximize the educational benefit realized from the considerable investment of resources necessary to operate and maintain these facilities.</li> <li>• Users who violate the policy shall be subject to disciplinary action including, but not limited to, written warnings, suspension without pay, or dismissal in accordance with the applicable provisions of the appropriate policy.</li> <li>• In addition, if a user's conduct violates federal or state laws, the user may be subject to prosecution under such laws.</li> <li>• Lee College reserves the right to investigate suspected violations using all means available.</li> <li>• Any abuse of Lee College WAN Network (LEEnet) by students, faculty, administrators or staff should be reported to the Office of Information Technology.</li> <li>• Users should be aware that the computer systems are the property of the College and e-mail messages, internet usage, and other computer files are subject to review at the discretion of Lee College. In the case of harassment complaints, illegal violations, or a system problem--hardware, software, or attacks by hackers--the IT staff is authorized to review any information or files necessary to investigate complaints or solve the systems problems to protect the systems and the information they contain. In this situation, the staff is obligated to treat any information they might see that turns out to be unrelated to the problem as strictly confidential. In addition, e-mail messages may be subject to subpoena or otherwise discoverable in litigation.</li> <li>• Users should follow local, state, and federal laws and regulations pertaining to computing activities. In cases involving fraud, forgery, extortion, copyright, intimidation, humiliation, etc., violators may be legally prosecuted and will be subject to immediate loss of all computing privileges at Lee College.</li> <li>• Attempt to alter or obscure your identity or your computer's identity, including but not</li> </ul>

- limited to IP address and email address, while communicating on any network.
- Attempts to alter system software, to bypass security protocols, to introduce viruses, worms, or other malicious or destructive programs, or otherwise “to hack” are expressly forbidden. Any member of the Lee College community, including students, who intentionally breaches security, will be subject to disciplinary action, including suspension and dismissal and legal proceedings.
  - The College District reserves the right to conduct searches when the College District has reasonable cause to believe that a search will uncover evidence of work-related misconduct. The College District may search the employee, the employee’s personal items, work areas, lockers and private vehicles parked on College District premises or worksites or used in College District business. Work areas include technology equipment provide by the college such as computers and peripherals, servers, laptops, PDAs and telephones/cell phones. (DHB Local: Employee Standards of Conduct: Searches).

For more information, see applicable laws and regulations:

Copyright: [http://www4.law.cornell.edu/uscode/html/uscode17/usc\\_sup\\_01\\_17.html](http://www4.law.cornell.edu/uscode/html/uscode17/usc_sup_01_17.html)

FERPA: [http://www4.law.cornell.edu/uscode/html/uscode20/usc\\_sec\\_20\\_00001232---g000-.html](http://www4.law.cornell.edu/uscode/html/uscode20/usc_sec_20_00001232---g000-.html)

*January 2006 – Office of Information Technology – Acceptable Use Policy*



## Office of Information Technology

[IT Home Page](#) | [Information](#) | [About IT](#) | [Support](#) | [PeopleSoft](#)

### Policy and Procedures

## Contractor Support Procedures

#### About IT

[Vision, Mission & Guiding Principles](#)

[2005-2006 Proposed Projects](#)

[IT Staff](#)

[Policies & Procedures](#)

[IT in Action \(Photos\)](#)

The purpose of this section is to provide procedures for the justification of all professional services contracts and any action regarding contract performance.

A performance evaluation of all contract employees should be a continuing ongoing activity occurring regularly through effective supervision in the process of communicating work assignments, monitoring activity, identifying requirements for improvements and critiquing the quality and quantity of contractor productivity.

### Lee College Service Letter of Agreement (SLA)

The agreement is between (Contractor Corporation Name) henceforth known as (contractor) and Lee College for computer repair and maintenance services. The (contractor) will obtain work requests through Information Technology and Telecommunication Services (ITT) workorder system from the Production Control Clerk. The contractor will be given access on the server to the standard software configurations for Lee College campus computers. Under no circumstances will the (contractor) install unlicensed software or work on non-tagged college equipment. The (contractor) will report to the Production Control Clerk prior to performing any work on campus, obtain workorder and proceed to work locations.

Lee College will provide contractor with a detailed workorder specifying: (a) work to be done, (b) specific location of job, (c) contract person, and (d) phone number. The (contractor) will provide documentation on each workorder of the work completed, software installed, parts used and any other services and/or training provided. The (contractor) will keep track of time for each workorder and fill out the appropriate sections for each work request. A detailed invoice will satisfy Lee College job tracking requirements. Time sheets must be completed and signed by the Director of Information Technology and Telecommunications Services. Subcontracted employees of (contractor) must abide by the rules and regulations of Lee College. The (contractor) must complete all workorders to the satisfaction of Lee College. Contractor shall notify Lee College promptly of any expected delay in performance beyond its reasonable control. Lee College may, at any time, make changes within the scope of work or period of performance of this contract.

### Client Site Protocol

Contractor employees must keep in mind during all contacts with client personnel (faculty, administrators, staff) that client satisfaction is paramount. Invoices will not be paid until all services have been satisfactorily performed. Contractor employee speech, actions, dress and attitude must not detract from client satisfaction at any time. The college encourages contractor employees to develop friendly business relationships with clients. Contractors must keep in mind, however that they are representing the Information Technology and Telecommunications Department in such contacts and avoid actions or speech that would reflect unfavorably on the department.

During the execution of this contract, contractor personnel reflect upon the Lee College. Contractor commits to maintaining high standards of professional conduct, neat and clean appearance of equipment and personnel, and honest business practices are required. Parties agree that poor attitude of personnel, misstatements on reports or invoices, talking negatively about ITT personnel are examples of unacceptable behavior. The contractor is expected to safeguard keys and passwords as well as equipment and parts utilized. The job site must be clean and the contractor must provide detailed documentation all work completed. The college shall retain the right to request the removal of any of the contractor's personnel at any time.



## Office of Information Technology

[IT Home Page](#) | [Information](#) | [About IT](#) | [Support](#) | [PeopleSoft](#)

### About IT

[Vision, Mission & Guiding Principles](#)

[2005-2006 Proposed Projects](#)

[IT Staff](#)

[Policies & Procedures](#)

[IT in Action \(Photos\)](#)

## Policy and Procedures

### E-Mail Guidelines

Lee College encourages appropriate use of E-Mail to enhance productivity through the efficient exchange of information in pursuit of education and research. Use of these resources must be consistent with the mission and goals of the college. As a responsible member of the college community, you are expected to act in accord with the following general guidelines.

Messages sent as electronic mail should meet the same standards for distribution or display as if they were tangible documents or instruments. Identify yourself clearly and accurately in all electronic communications. Alteration of the source of electronic mail, message or posting is unethical and possibly illegal.

Be sensitive to the inherent limitations of shared network resources. No computer security system can absolutely prevent a determined person from accessing stored information that they are not authorized to access.

1. Be considerate. Too much information in one message is a burden on recipients. Screens are harder to read than words on paper.
2. Don't send junk mail. Refrain from using E-Mail for unnecessary broadcasting. For example, chain letters are an inappropriate use of E-Mail and can cause excessive loading of mail facilities.
3. Assume the messages you send and receive are permanent; therefore, don't say anything in E-Mail that you might not want to be made public or forwarded to others.
4. Be aware that E-Mail might not be as private as you may wish because it works through shared technology. If confidentiality and privacy are very important, it may be advisable and more appropriate to use other communication methods.
5. Cite your information clearly and correctly, even if you are paraphrasing. If you are sending information from another source, pay attention to whether the material is copyrighted. Copyright laws apply to E-Mail as well as to printed media.
6. Don't forward confidential mail to others without first obtaining permission.
7. Don't expect instant response to your mail. Not everyone anxiously awaits your message. If you are uncertain of a recipient's E-Mail habits or are not getting any response to your message, a phone call or memo may be quicker and more effective.

Sources:

Abridged from Business Communication Quarterly (September 1995). University of Texas at Austin E-Mail Policy (April, 1994).



# LIBRARY

ERMA WOOD CARLSON

281/425-6379  
Toll free: 800/261-9556  
Reference Desk: 281/425-6584

1ST FLOOR  
ADVANCED TECHNOLOGY CENTER

[Ask a Librarian](#) | [Help](#) | [Virtual Tour](#) | [New Acquisitions](#) | [Comments](#) | [Catalog](#) | [Article Databases](#)

## About

[Our Library](#)

[Hours](#)

[Staff](#)

[Contact Information](#)

[Printing/Copying in the Library](#)

[Library Policies](#)

[Computer Use](#)

[Library Goals & Report Card](#)

## Library Acceptable Use Policy

The Internet is a global entity with a highly diverse user population and information content. It offers access to many valuable local, national, and international sources of information. It is the individual's responsibility to exercise judgment and evaluate both the content and validity of information just as they would any printed publication.

Lee College Library provides access to the Internet and expects that all who exercise the privilege of this access will do so responsibly. These guidelines are developed to clarify the Lee College Library position regarding Internet access and guidelines for persons accessing the Internet through the library's computers.

Lee College Library assumes responsibility for the accuracy of the information provided on its home page.

- The Library does not censor access to materials or protect users from materials they may find offensive.
- The Library does not accept responsibility for the content of sites accessible through the Internet, nor is it responsible for content of sources accessed through secondary links.
- Access to the Internet via the Library's workstations is both a service and a privilege extended to all current Lee College students, faculty, staff and adult service area residents.
- The Library encourages the educational and personal use of the World Wide Web consistent with the college's [Acceptable Use Policy](#).

### Guidelines

All users of the Library Internet workstations are expected to abide by the following guidelines. Violation of these guidelines may result in Internet privileges being revoked.

- Priority use is for those who have course-related needs and patrons may be asked to yield to

those with those needs. No chatting or games

- If you are taking a class at Lee College that requires access to e-mail and you are communicating with your instructor for classes, you have unlimited access. If you are accessing e-mail for any other purpose we ask that you limit your time to 15 minutes.
- Posted time limits may be implemented if others are waiting to use the computer.
- Patrons are to refrain from performing any act that will impair the operation of any facet of access to the Internet or configuration of the workstations. No changing workstation settings.

## **Illegal Use**

Patrons must refrain from any use of Internet resources which is illegal in Texas, any other state or the United States. Therefore Internet patrons at Lee College Library must refrain from displaying or distributing material in any format which is in anyway inconsistent with Lee College's Acceptable Use Policy. Federal laws governing the Internet state: "it is illegal to access via the Internet any material that violates state or federal laws." For example, 18 U.S. Code 2252 forbids the sexual exploitation of children, including child pornography.

Each person using the Internet computers of the Lee College Library is liable for any infringement and is subject to criminal prosecution for illegal use. Lee College monitors its public access computers. Any illegal use will be reported. Please be prepared to show ID upon request.

## **Copyright**

Copyright Law (title 17, U.S. Code) prohibits the unauthorized reproduction or distribution of copyrighted materials, except as permitted by the principles of "fair use". Patrons may not copy or distribute electronic materials (including electronic mail, text, images, programs or data) without the explicit permission of the copyright holder.

Any responsibility for any consequences of copyright infringement lies with the user; the Library expressly disclaims any liability or responsibility from such use. The Library expressly disclaims any liability or responsibility arising from access to or use of information obtained through its electronic information systems, or any consequences thereof.

*Updated: December 2003*



## Office of Information Technology

[IT Home Page](#) | [Information](#) | [About IT](#) | [Support](#) | [PeopleSoft](#)

### About IT

[Vision, Mission & Guiding Principles](#)

[2005-2006 Proposed Projects](#)

[IT Staff](#)

[Policies & Procedures](#)

[IT in Action \(Photos\)](#)

## Policy and Procedures

### Using Software

#### ***A Guide to the Ethical and Legal Use of Software for Members of the Lee College District***

Software enables us to accomplish many different tasks with computers. Unfortunately, in order to get our work done quickly and conveniently, some people make and use unauthorized software copies. The purpose of this information is to provide a brief outline of what you legally can and cannot do with software. Hopefully, it will help you better understand the implications and restrictions of the U.S. Copyright Law.

#### **Here Are Some Relevant Facts:**

UNAUTHORIZED copying of software is illegal. Copyright law protects software authors and publishers, just as patent law protects inventors.

UNAUTHORIZED copying of software by individuals can harm the entire academic community. If unauthorized copying proliferates on a campus, the institution may incur legal liability. Also, the institution may find it more difficult to negotiate agreements that would make software more widely and less expensively available to members of the Lee College community.

UNAUTHORIZED copying and use of software deprives publishers and developers of a fair return for their work, increases prices, reduces the level of future support and enhancements and can inhibit the development of new software products.

RESPECT for the intellectual work of others has traditionally been essential to the mission of colleges and universities. As members of the Lee College District, we value the free exchange of ideas. Just as we do not tolerate plagiarism, we do not condone the unauthorized copying of software, including programs, applications, databases and code.

THEREFORE, we offer the following statement of principle about intellectual property and the legal and ethical use of software.

#### **The EDUCOM Code**

#### **Software and Intellectual Rights**

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy, and right to determine the form, manner and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and

trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

## Classification of Software

In terms of copyright, there are four broad classifications of software, however, Information Technology and Telecommunication Services provides a fifth classification:

- Commercial Software
- Shareware
- Freeware
- Public Domain
- Site Licensed

The restrictions and limitations regarding each classification are different.

### COMMERCIAL

Commercial software represents the majority of software purchased from software publishers, commercial computer stores, etc. When you buy software, you are actually acquiring a license to use it, not own it. You acquire the license from the company that owns the copyright. The conditions and restrictions of the license agreement vary from program to program and should be read carefully. In general, commercial software licenses stipulate that

1. the software is covered by copyright,
2. although one archival copy of the software can be made, the backup copy cannot be use except when the original package fails or is destroyed,
3. modifications to the software are not allowed,
4. decompiling (i.e., reverse engineering) of the program code is not allowed without the permission of the copyright holder, and
5. development of new works built upon the package (derived works) is not allowed without the permission of the copyright holder.

### SHAREWARE

Shareware software is covered by copyright, as well. When you acquire software under a shareware arrangement, you are actually acquiring a license to use it, not own it. You acquire the license from the individual or company that owns the copyright. The conditions and restrictions of the license agreement vary from program to program and should be read carefully. The copyright holders for shareware allow purchasers to make and distribute copies of the software, but demand that if, after testing the software, you adopt it for use, you must pay for it. In general, shareware software licenses stipulate that

1. the software is covered by copyright,
2. although one archival copy of the software can be made, the backup copy cannot be used except when the original package fails or is destroyed,
3. modifications to the software are not allowed,
4. decompiling (i.e., reverse engineering) of the program code is not allowed without the permission of the copyright holder, and
5. development of new works built upon the package (derived works) is not allowed without the permission of the copyright holder.

Selling software as shareware is a marketing decision, it does not change the legal requirements with respects to copyright. That means that you can make a single archival copy, but you are obliged to pay for all copies adopted for use. To continue to use shareware beyond its initial evaluation period without registering it (paying the vendor for it) is illegal.

## **FREWARE**

Freeware also is covered by copyright and subject to the conditions defined by the holder of the copyright. The conditions for freeware are in direct opposition to normal copyright restrictions. In general, freeware software licenses stipulate that

1. the software is covered by copyright,
2. copies of the software can be made for both archival and distribution purposes but that distribution cannot be for profit,
3. modifications to the software is allowed and encouraged,
4. decompiling (i.e., reverse engineering) of the program code is allowed without the explicit permission of the copyright holder, and
5. development of new works built upon the package (derived works) is allowed and encouraged with the condition that derivative works must also be designated as freeware. That means that you cannot take freeware, modify or extend it, and then sell it as commercial or shareware software.

## **PUBLIC DOMAIN**

Public Domain software comes into being when the original copyright holder explicitly relinquishes all rights to the software. Since under current copyright law, all intellectual works (including software) are protected as soon as they are committed to a medium for something to be public domain it must be clearly marked as such. Before March 1, 1989, it was assumed that intellectual works were NOT covered by copyright unless the copyright symbol and declaration appeared on the work. With the U.S. adherence to the Berne Convention this presumption has been reversed. Now all works assume copyright protection unless the public domain notification is stated. This means that for public domain software

1. copyright rights have been relinquished,
2. software copies can be made for both archival and distribution purposes with no restrictions as to distribution,
3. modifications to the software are allowed,
4. decompiling (i.e. reverse engineering) of the program code is allowed, and
5. development of new works built upon the package (derivative works) is allowed without conditions on the distribution or use of the derivative work.

## **SITE LICENSED**

Site Licensed software is copyrighted software that has been licensed for usage on campus. The conditions and restrictions of the license agreement vary from program to program and should be read carefully. In general, site licensed software licenses stipulate that

1. the software is covered by copyright,
2. although one archival copy of the software can be made, the backup copy cannot be use except when the original package fails or is destroyed,
3. modifications to the software are not allowed,
4. decompiling (i.e., reverse engineering) of the program code is not allowed without the permission of the copyright holder, and
5. development of new works built upon the package (derived works) is not allowed without the permission of the copyright holder. The specifics of usage and distribution of site licensed software are determined in the license agreement. For specific information on a license agreement, contact Information Technology and Telecommunication Services at Lee College.

## **FAQ's about Using Software**

*What do I need to know about software and the U.S. Copyright Act?*

It's really very simple. The Copyright Law recognizes that all intellectual works (programs, data, pictures, articles, books, etc.) are automatically covered by copyright unless it is explicitly noted to the contrary. That means that the owner of a copyright holds the exclusive right to reproduce and distribute his or her work. For software this means it is illegal to copy or distribute software, or its documentation, without the permission of the copyright holder. If you have a legal copy of software you are allowed to make a single archival copy of the software for backup purposes. However, the copy can only be used if the original software is destroyed or fails to work. When the original is given away, the backup copy must also be given with the original or destroyed.

*If software is not copy-protected, do I have the right to copy it?*

Lack of copy-protection does NOT constitute permission to copy software without authorization of the software copyright owner. "Non-copy-protected" software enables you to make a backup copy. In offering non-copy-protected software to you, the developer or publisher has demonstrated significant trust in your integrity.

*May I copy software that is available through facilities on my campus, so that I can use it more conveniently in my own office or classroom?*

Software acquired by colleges and universities is usually covered by licenses. The licenses should clearly state how and where the software might be legally used by members of the relevant campus communities (faculty, staff and students). Such licenses cover software whether installed on stand-alone or networked systems, whether in private offices and rooms or in public clusters and laboratories. Some institutional licenses permit copying for certain purposes. The license may limit copying, as well. Consult with the Director of Information Technology and Telecommunication Services if you are unsure about the permissible use of a particular software product.

*May I loan software?*

The 1990 modification to the Copyright Law makes it illegal to "loan, lease or rent software" for purposes of direct or indirect commercial advantage without the specific permission of the copyright holder. Non-profit educational institutions are exempted from the 1990 modification, so institutional software may be loaned. Some licenses may even restrict the use of a copy to a specific machine, even if you own more than one system. In general, licenses usually do NOT allow the software to be installed or resident on more than a single machine, or to run the software simultaneously on two or more machines.

*Can I bring software in from home or from a friend and installed it on my office computer?*

You may bring software in from home or from a friend and installed it on your office computer as long as you have a license for the software. In addition, the original license (not a copy of the license) must be visible and in the same location as the computer. We conduct annual audits of Lee College serial number tagged computer equipment and we must verify that the software on the computer is legal. Remember, the office computer belongs to the institution and is subject to the same policy and procedures that govern institutional property.

*May I install software from my office computer on my home computer?*

Software installed on office computers is licensed to the college. You may not install software from your office computer to home. Software agreements and contractual software licenses purchased by the college are for educational uses only. Users are expected to abide by these agreements which prohibit copying programs or data for use on other systems.

*Isn't it legally "fair use" to copy software if the purpose in sharing it is purely educational?*

Historically, the Copyright Law was modified to permit certain educational uses of copyrighted materials without the usual copyright restrictions. However, "fair use" of computer software is still a cloudy issue. The "fair use" amendments to the copyright law are intended to allow educational use of legally protected products, but it is limited (for paper-based products) to small portions of full works. For most software it is clearly illegal to make and distribute unauthorized, fully-functional copies to class members for their individual use. Making copies of a small section of code from a program in order to illustrate a programming technique might not be a violation. The best alternative is to clear any such use with the copyright owner or consult the appropriate authorities at your institution.

### **Alternatives To Explore**

Software can be expensive. You may think that you cannot afford to purchase certain programs that you need. Site-licensed and bulk-purchases software are legal alternatives that make multiple copies of software more affordable. Many educational institutions negotiate special prices for software used and purchased by faculty, staff and students. Consult your campus computing office for information. As with other software, site-licensed or bulk-purchased software is still covered by copyright, although the price per copy may be significantly lower than the normal commercial price. A usual condition of site-licensing or bulk-purchasing is that copying and distribution of the software is limited to a central office, which must maintain inventories of who received it. When you leave the academic community by graduation, retirement or resignation, you may no longer be covered by the institutional agreement and may be required to return or destroy your copies of the software licensed to the institution. The Lee College District requires you to return any software licensed to the institution. Many colleges sell software through a campus store at "educational discounts." If you purchase software for yourself (not with institutional funds) through such an outlet, the software is yours and need not be destroyed or surrendered when you leave the institution. It is, however, still covered by normal copyright protection and covered by the specific conditions of the licensing agreement.

### **A Final Note**

Restrictions on the use of software are far from uniform. You should check carefully each piece of software and the accompanying documentation yourself. In general, you do not have the right to:

- Receive and use unauthorized copies of software, or
- Make unauthorized copies of software for others.

If you have questions not answered by this information about the proper use and distribution of a software product, seek help from the Information Technology and Telecommunication Services Department, the software developer or publisher.

This information has been produced as a service to the Lee College District by the Information Technology and Telecommunication Services of Lee College, Educational Uses of Information Technology Program (EUIT) of EDUCOM and the Information Technology Association of America (ITAA). EDUCOM is a non-profit consortium of colleges and universities committed to the use and management of information technology in higher education. ITAA is an industry association providing issues management advocacy, public affairs, business-to-business networking, education and other member services to companies, which create, and market products and services associated with computers, communications and data.





## **Virtual Private Network (VPN) Policy**

### **Office of Information Technology Division**

#### **1.0 Introduction**

In an effort to increase the security of Lee College's information technology systems, off campus access to many information technology resources has been limited. Lee College offers Virtual Private Network (VPN) access for faculty/staff (hereinafter users) who need access to information technology systems that are not available to users from off-campus networks. Exceptions to the approved list of users will be considered on a case by case basis. The President and Deans will approve the list of users.

#### **2.0 Purpose**

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to Lee College's internal network. Lee College's VPN server is designed to provide secure/encrypted access to network resources on the Lee College Network. Using the VPN server to access Internet resources external to Lee College is not recommended.

#### **3.0 Policy**

**3.1** VPN gateways will be set up and managed only by Lee College Office of Information Technology Networking Services Group.

**3.2** Approved users laptops will be configured with the VPN client software by technicians at Lee College Office of Information Technology division.

**3.3** Only VPN client software that is approved by and/or distributed by the Office of Information Technology networking services may be used to connect to the Lee College VPN concentrators.

**3.4** By using VPN technology with personal equipment, users must understand that their machines are an extension of Lee College's network, and as such must comply with Lee College's Information Technology Policies <http://www.lee.edu/itt/accusepol.asp>.

**3.5** VPN provides secure access into the Lee College Network. VPN does not, by itself, provide Internet connectivity. Users are responsible for providing their own Internet service via dial-up, cable modem, DSL, or other means to be able to use Lee College's VPN service.

**3.6** Currently VPN software is available for Windows 2000/XP and Mac OS X. Approved users are responsible for the installation of the VPN software.

**3.7** It is the responsibility of the users with VPN privileges to ensure that unauthorized persons are not allowed access to Lee College internal networks.

**3.8** Lee College has configured the VPN service to not allow the bridging of networks (split tunneling). As a result, when connected to VPN, all network traffic from the users' computer will travel through the Lee College network which will not allow communication back to a device on the private network other than the computer making the original connection.

**3.9** All computers, including personal computers, connected to Lee College's internal networks via VPN or any other technology must use the most up-to-date anti-virus software approved by the College.

**3.10** VPN users will be automatically disconnected from Lee College's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes should not be used to keep the connection open.

**3.11** Only one active VPN connection is allowed per user and the VPN concentrator is limited to a total connection time of 8 hours per user in one session.

**3.12** Only approved users with signatures from the Dean and/or President with specific requirements for VPN access will be granted access to the resources.

#### **4.0 Enforcement**

Any user found to have violated this policy may be subject to loss of certain privileges or services, including but not necessarily limited to loss of VPN services.



**By acceptance of VPN (virtual private network) access, I certify that I have read, understand and agree with the policy and procedures set forth in this document. Return signed document to Office of Information Technology.**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Dean/President: \_\_\_\_\_ Date: \_\_\_\_\_

OIT: \_\_\_\_\_ Date: \_\_\_\_\_