Acceptable Use Policy

Information Resources

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 (See Board of Regents). 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 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.
- 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.

Data Protection Copyright

- 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.
- 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.
- 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).
- 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.
- 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 Title 17, United State Code).
- 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.

- 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 CDs is **illegal**.
- 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: http://www.lee.edu/catalog.asp.

Virus Protection

- All computers connecting to the Lee College network must run current site-licensed virus prevention software.
- Centrally provided virus protection software must be run on all computers connected to the Lee College network.
- 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.
- 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.
- 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.
- 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.

Email

- The following email activities are prohibited by policy:
  - Using email for purposes of political lobbying or campaigning.
  - Posing as anyone other than oneself when sending email.
  - Reading another User's email unless authorized to do so by the owner of the email
  - Using email software that poses high security risks to Lee College Information Resources.
  - Sending unsolicited messages, except as required to conduct Lee College business.
  - Sending excessively large messages or attachments unless for office College business.
  - Sending or forwarding email that is likely to contain computer viruses.
- 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.
- 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.
- Initiating or forwarding chain letters or email is prohibited on the college email systems and the Internet as a whole. Chain emails can be identified by phrases such as "please pass this on to your friends" or similar inducements that encourage you to forward the message.
- 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 (instant-messaging and peer to peer technologies) are often used by intruders with malicious intent. Non-business-related instant-messaging should be avoided.
- Address messages to recipients who need to know. Messages sent unnecessarily to a long list of recipient's lowers system performance.
- 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.
- The use of email or any college system for harassment or criminal activity may result in criminal penalties, including fines and imprisonment.

Use of Information Resources

- 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 percent of a user's allocated mailbox space) unless stored on the hard drive or external media.
- 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.
- Non-work related files may not be stored on network file servers.
- 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.
- Commercial network resources and software that are licensed by Lee College for internal use only may not be used outside the College network.

Internet Use

- 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.
- To ensure 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 that may have adverse legal implications for Lee College is discovered, it will be reported.

- Neither personal nor commercial advertising may be posted on Lee College websites.
- Users shall not engage in activities that relate to material involving the sexual exploitation of minors as defined by Federal Code Title 18, Part I, Chapter 110, Sexual Exploitation and other abuse of children or other criminal acts.

Portable and Remote Computing

- 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.
- 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 IT minimum standards for portable computing, and are subject to the same rules and security related requirements that apply to college owned computers.
- All hardware that connects to the Lee College network must be installed by certified Office of Technology technicians and network administrators.

Passwords

- Lee College account(s), passwords, personal identification numbers (PINs), security tokens (i.e., Smartcards), 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, usernames and passwords.
- Digital certificate passwords used for digital signatures must never be divulged to anyone.
- Users must not circumvent password entry through use of auto login, application “remember password” features, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (such as automated backups) with the approval of the Lee College Office of Information Technology director. Any exception situation must include a procedure to change the passwords and must adhere to security policies for password construction.
- 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.
- Users must establish appropriate passwords, change them as required and never share them with others.

Telephone Long-Distance Access Code

- Users shall not tap phone/data lines or accessing files by circumventing security restrictions.

- 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.
- Telephone services and wiring may not be modified or extended beyond the area of their intended use.
- 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.
- 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).
- 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).

CyberSecurity

- 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 Information Technology.
- 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 email 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.
- 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.
- 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.
- 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 Director prior to activating any such service.
- 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.

- 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.
- 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 dial-up 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.
- 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.
- 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.

Your Rights and Responsibilities

- 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.
- 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.
- 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.

Violations of AUP

- 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.

- Policies and guidelines are established to maximize the educational benefit realized from the considerable investment of resources necessary to operate and maintain these facilities.
- 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.
- In addition, if a user’s conduct violates federal or state laws, the user may be subject to prosecution under such laws.
- Lee College reserves the right to investigate suspected violations using all means available.
- Any abuse of Lee College WAN by students, faculty, administrators or staff should be reported to IT.
- Users should be aware that the computer systems are the property of the College and email 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, email messages may be subject to subpoena or otherwise discoverable in litigation.
- 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.
- Attempt to alter or obscure your identity or your computer’s identity, including but not 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 work sites 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).