



LUBBOCK
CHRISTIAN
UNIVERSITY

*the
Life
Changing
University*

POLICY AND
PROCEDURES
Number: 6.1
Page: 1 of 11
Revised: 09-05-2018

Policy and Procedure: Acceptable Use of Technology Resources

INTRODUCTION

The mission of the Lubbock Christian University Technology Services Department is to empower collaboration and communication to achieve academic and administrative excellence through the strategic use of people, processes, and technology. The department's key goals and objectives direct how computing equipment, networks, systems, software, printing, and telephones (Technology Resources) will be employed to improve instructional systems, information systems, and communications services. Technology Resources play a key role in enhancing academic programs and supporting services available to faculty, staff and students (clients). The leadership of the Technology Services Department (Technology Services) functions as the agent of the University in matters related to all university technology resources.

This policy is formulated to create an environment where the clients, as users of the university technology resources, have an understanding of their responsibilities, duties and obligations to ensure the university technology resources are used only in a manner consistent within the mission of the University.

Information Systems have greatly expanded our ability to access and exchange information, and represent rich resources for innovation in the continuance of LCU's mission. The wise use of these technologies require a vigilant effort with special attention to security safeguards effected to protect individual rights of privacy.

This document contains specific rules for appropriate behavior when using LCU Technology Resources. Its purpose is to condense and present the LCU policies in plain language.

SCOPE

These rules apply to all users of Technology Resources, Technology equipment owned, leased or rented by Lubbock Christian University as well as user owned, leased or rented equipment connected to University Technology Resources. Users includes, but is not limited to:

- Students,
- Academic staff,
- Visiting academic staff,
- Administrative staff, • Guests of the University and
- Vendors or organizations.

Technology Resources includes, but is not limited to:

- Microcomputers in offices,
- Network Printers and Copiers,

- Locally attached printers
- Telephone equipment
- University computer labs,
- Library computers,
- Servers,
- Networking equipment and services used to link these components together and to the Internet, • Offsite Services owned or contracted for University use.
- Portable devices

By utilizing LCU technology credentials and resources you agree that you are in compliance with all state, national and international copyright, other intellectual property laws and agreements and other related laws. Furthermore, you agree to compensate, exonerate and protect the University (and its representatives) for any claim, damage or cost related to your use of the University's Technology Resources.

FREE AND OPEN USAGE

The University's Technology environment is dynamic, characterized by responsible openness, creativity and free sharing of information. This policy respects this environment and limits these characteristics when necessary to protect the mission of Lubbock Christian University and in upholding Christian principles.

AUTHORIZED USAGE

LCU Technology Services will determine who has access to available technology resources. These resources connect to a variety of services available on the campus intranet, as well as services offered across the internet. Clients are authorized to access resources appropriate to their job. Students are authorized to access resources for academic purposes relating to their course of study at the University. All clients have a responsibility to use the technology resources in a responsible and considerate manner that will allow everyone to benefit from the University's infrastructure investments. Clients are required to respect the LCU mission and vision and abide by all University policies and codes of conduct. As a technology resource user, you agree to the following rules:

1. You are responsible for any user account you have been given. You shall set a password on the account that is not easily guessed and in compliance with the password complexity requirements as established by Technology Services. You shall not share this password with any other person. If you discover that someone has made unauthorized use of your user account, you shall immediately change your password and report the event to one of the individuals listed in Appendix A. You also agree not to use an account that has not been assigned to you by Technology Services.
2. You agree not to copy or modify password files without permission, other users' files, data storage belonging to other users, or seek confidential information about other users, whether at LCU or any other organization.
3. You shall not attempt to decrypt material which you are not entitled to nor attempt to gain rights you have not been specifically granted by the owner. If you observe or discover a breach in system security, you agree not to exploit the breach and to inform the Technology Services security coordinator (listed in Appendix A) immediately.
4. You agree to refrain from any intentional activity that interferes with a computer's operating system or its logging and security systems, or that may cause such effects.
5. You agree not to install or use unauthorized file-sharing programs on the LCU network. Use of these programs introduces security breaches and copyright violations.

6. You shall be sensitive to the public nature of computer systems and refrain from transmitting, posting or otherwise displaying material that is threatening, obscene, discriminating, harassing, defamatory or contrary in any way to the mission and vision of Lubbock Christian University.
7. You agree not to make copies of or distribute software owned or licensed by the University. If the owner of the software or the owner of the license has specifically granted permission to make copies then you may do so. If in doubt as to whether you have permission to copy software, assume you do not!
8. Messages, statements and declarations sent as electronic mail or public postings are treated as if they were tangible documents. In a manner similar to how letterhead or a return address on a tangible document would identify the University, electronic mail headers can see that the University is the source of the message and that the University system is being used to transmit the messages.
9. You agree not to create, alter or delete any electronic information contained in any system associated with the University Technology Resources that is not part of your own work.
10. You agree not to create, send or forward electronic chain mail letters. You agree not to attempt to alter or forge the "from" line or any other provenance contained in electronic mail or postings.
11. You shall not use LCU Technology Resources as a means of obtaining unauthorized access to any other computing systems.
12. LCU's computing disk storage is a University resource with costs attached and is to be used with care and discretion. It is not meant to be used for archiving programs and data not currently being used or for storage of files publicly available elsewhere. It is meant for current class work, research and development projects, and temporary storage of other files. You shall attempt to keep your disk usage minimized and will refrain from maintaining duplicate copies of software already installed on the system.
13. Network addresses, such as TCP/IP addresses, are assigned by Technology Services and may not be altered or otherwise assigned without the explicit permission of Technology Services. No equipment may be attached to the technology resources without the explicit permission of the Technology Services.
14. You agree not to use the system for business unrelated to the University such as the transmission of commercial or personal advertisements, solicitations and promotions, or for reproduction of political or commercial material.
15. You agree to use the University telephone facilities in an appropriate, legal manner. The telephone system is not to be used in a threatening or harassing manner. All long distance access codes are to be protected from unauthorized use.
16. The use of non-LCU owned or leased equipment connected to LCU owned or leased equipment or the network is not supported by TS. If problems or interference occurs the non-LCU equipment will be restricted. This includes portable devices, printers, cameras, scanners, disk duplicators, projectors, and other such equipment.
17. Operating systems will be upgraded on faculty and staff machines only where it can be demonstrated that the upgrade is necessary to conduct LCU business, or a recurring problem that prevents LCU related business from being conducted can be corrected. Operating systems will be upgraded when hardware is upgraded or replaced.
18. The use of software that is not licensed by LCU on LCU owned or leased equipment without prior authorization is strictly forbidden.
19. You agree to not transmit through unsecured electronic media communications that contain any combination of student names, social security numbers, birth dates, or other personal information

in a way that would lead to a breach of FERPA. Unsecured electronic media includes, but is not limited to email, text messaging and social media.

20. You agree to not transmit through unsecured electronic media communications that contain credit card numbers or bank account numbers or other financially identifying information that would lead to a breach of trust. Unsecured electronic media includes, but is not limited to email, text messaging and social media.

Access may be denied to any person who has a history of abuse of university technology resources or other technology services. Abuses of these privileges will lead to action in accordance with the Lubbock Christian University Student Handbook and/or the Lubbock Christian University Employee Handbook.

AUTHORIZED CLIENTS

Access to the University's technology resources is for authorized faculty, staff and students. Clients are responsible for their own accounts and are permitted to access only those resources for which they have been authorized. No client will use any other client's authorization to access any system or allow any other person to use his or her authorization to access any system. Under special circumstances people other than University faculty, staff and students will be granted access to technology resources. This access is granted with appropriate authorization with the understanding that all University technology resource policies will be obeyed. Special circumstance authorization is temporary. Access will be revoked as soon as circumstances that warranted the access have changed

REGISTRATION OF CLIENTS

These procedures only consider access to services requiring client registration:

- Employees may be authorized to access Technology Resources identified as being required to perform their duties, provided this is in accordance with other University policies, and subject to employment being confirmed by the University's personnel officer.
- Students may be registered to access computer laboratories and dorm network facilities, and to access a common set of electronic services that will provide them with an information rich learning environment. Students may be registered as users of other technology resources, provided it is a genuine requirement of their academic studies, or authorized by their instructors as being required to complete their studies, subject to authorization being confirmed by the University's technology services delegate.
- Campus Guests may use the campus guest level wireless access for lawful internet related use. No internal systems or logins will be will available at the guest level.
- Third Parties may be authorized as follows.
 1. Invited technicians, presenters, and collaborators to the University may be authorized to access technology resources in accordance with other University policies, and subject to:
 2. The authorization of the Director of Technology or delegated personnel.
 3. A campus employee taking the responsibility for monitoring and observing the work.
 4. The person's signed, emailed, or electronically signed acknowledgement to abide by the University's policies relating to the use of technology resources.
 5. Subject to authorization being confirmed by the University's delegated technology team members and/or the support or academic department seeking third party technology services.

USE OF UNIVERSITY PROPERTY

The University's technology resources, as with other University resources, are not to be used for purposes other than those considered appropriate by the University. Technology Resources are provided primarily to support the mission of the University. Limited personal use of the technology resources such as electronic communications and personal research are permitted provided the activity does not violate technology resource use policies or overburden the technology resources. If personal use of technology resources creates a problem on the network personal use will be restricted.

TELEPHONE

- All telephone service are provided through Technology Services. All requests for additional lines, repair of service, or termination of service is handled by Technology Services.
- When necessary long distance codes are provided by Technology Services.
- Access for international calling must be requested through Technology Services. Access will be limited to specific telephones.

PRINTING SERVICES

- Technology services provides access to network printers in each building on the LCU main campus. The network printers will be maintained by TS and all problems and service requests must be made to TS.
- All printing and copying activity is logged and logs are maintained by TS. Charges for use of network copiers and printers are allocated to each department on a monthly bases.
- Students are provided access to network printers and copiers. All charges for use are deducted from their personal account at the time of use. Statements can be provided upon request.
- Personal printers (those connected directly to the pc, not the network) are not supported by TS. Maintenance, supplies and replacement of personal printers will be the responsibility of owner (department, employee who purchased/provided printer, etc.).
- Addition of network printers and copiers will be determined by Technology Services.

SECURITY

Operational security of the institutional information system is based upon both physical security and adherence to standards. Technology Services maintains the authority for the establishment and enforcement of University standards for administrative programming code, machine access, program access, and maintenance (code and equipment).

The University's Technology Resources use individual user accounts and access credentials. It is the client's responsibility to ensure that:

- Credentials are selected in compliance with the credential complexity requirements as established by Technology Services. Credentials are not shared with other persons, computer workstations are kept physically secure, computer accounts are not shared with other persons, and long distance codes are kept secure.
- Clients will not take any action which would or might lead to circumventing or compromising security of any of the University's Technology Resources.
- Client will not take any action, which would or might lead to denial or impairment of access to, or effective use of, any Technology resource by any other authorized client.
- The circulation of software viruses, malware, spyware or similar malicious software is expressly forbidden.

- Any portable devices that are owned or used for LCU related work include a password before the device can be unlocked for use in case they are lost or stolen.

Use every available method to safeguard your data, including regular changes of account credentials and making duplicates of files. In the event that your files have been corrupted as a result of intrusion, notify the Technology Services immediately (details in Appendix A). Please note that computer systems are not completely secure. It is possible that others will be able to access files by exploiting shortcomings in the system security. For this and other reasons, LCU cannot guarantee confidentiality of files and other transmissions.

Technology Services attempts to provide reasonable security against damage to files stored on LCU's central file storage by making backups of files at regular intervals. In the event of lost or damaged files, a reasonable attempt will be made to recover the information. However, the University and Technology Services staff cannot guarantee recovery of the data. Technology Services recommends that clients make personal backups of important personal files on secure removable media.

Technology Services will make reasonable attempts to provide error-free hardware and software on University systems.

PHYSICAL SECURITY

Security is a physical problem as well as one of control of account credentials and other security measures. Security for equipment assigned to locations not controlled by Technology Services is the responsibility of the department where the equipment is located. Portable devices such as laptops, tablets, and other components designed for portability are designated under the control of the department member the employee works. That department is expected to have awareness of general location of components included in LCU inventory.

Unauthorized removal of University equipment not designed for portability from the assigned location to another University location may constitute a security violation. Check with Technology Services before moving this equipment. An off-campus permit obtained through Technology Services is required before any University computer not designated for portability may be removed from campus.

PRIVACY

Lubbock Christian University attempts to maintain privacy of client files and communications. All Email addresses associated with the lcu.edu domain are licensed and assigned supervision to Lubbock Christian University. Third parties such as Microsoft and any number of providers that employees might send email to can be involved in routing and holding email and related file communication. As such, Technology Services reserves the right and has the responsibility to examine files and directories associated with LCU operations for the reasons listed below but not limited to:

- System integrity is or may be threatened.
- Security is compromised.
- An activity has a detrimental impact on the quality of service to other clients.
- The system is being used for purposes which are prohibited.
- The system is being used for unlawful purposes.
- System backups, which access all files in your account.
- Software upgrades, which may require editing startup files in your account.

- Diagnostic and trouble-shooting activities, which may, for example, require viewing the address headers of your e-mail messages to determine the cause of problems.
- Keystroke Monitoring of sessions to determine inappropriate use of the computing resources.
- Suspected violation of LCU policy or law. If there is sufficient cause to suspect such a situation, your files will be duplicated and stored without your permission for review by appropriate personnel.

Exercise caution when storing any confidential information in electronic format. Technology Services staff are expected to respect the confidentiality of electronic information and shall not log into your account or access your files unless specifically granted permission by you. Exceptions to this guideline are made under certain circumstances.

In the event that your files need to be copied or viewed for reasons other than security, diagnostic, system backup or in compliance with law enforcement, Technology Services staff will attempt to inform you of this access.

Student staff are not to be involved in situations where helping another student or a faculty member would give them access to data relevant to a course that the student staff person is currently taking.

USE OF COOKIES

Cookies are files containing information which is downloaded to user devices when visiting a website to enable the site to recognize user devices. Cookies can be combined to create profiles that can be used to create user profiles. Use of cookies to create user profiles require user consent, and the data subject must have the right to withdraw consent. Internal university sites do not normally use cookies to create user profiles. Employees using third party providers must evaluate cookie use to ensure it is consistent with university policy and complies with applicable laws.

STANDARD OFFICE COMPUTING ENVIRONMENT

Technology Services has adopted a standard suite of office applications software to provide benefits to the University community in the form of improved communications, training materials and technical support services for clients with workstation connections to the campus network.

Standards for use and purchase of University-owned computer software are established to economically and efficiently coordinate computing activities. Technology Services manages all software purchases to assure compatibility with University uses, support, and software purchasing and licensing procedures.

COPYRIGHT LAWS

Copyright is intended to provide protection of the "intellectual property" for original content.

The use of a copyrighted image, sound or video in a presentation; copy material produced by another person; use copyrighted text in a document; or make an extra copy of a computer program, is a copyright infringement.

Two terms that you may come across with regard to software copyright are shareware and public domain.

SHAREWARE

Shareware is software with usually limited capability or incomplete documentation which is available for trial use at little or no cost but which can be upgraded upon payment of a fee to the author.

The software will usually contain a message that indicates where you send your fee or "registration". The author retains copyright of the software. Most shareware authors will send you updated or enhanced versions of the product once you are registered.

PUBLIC DOMAIN

Public domain software is available free of charge and can be copied and distributed freely. However, copyright still applies to public domain software. Therefore, if you modify and redistribute public domain software, you must obtain permission and acknowledge the original authors.

The copyright laws provide strong legal protection against unauthorized copying or use of computer software with heavy penalties that apply to individuals and organizations who breach these laws.

In brief, it is illegal:

- To copy or distribute software or any accompanying material without the permission or license from the copyright owner;
- To run a copyrighted software program on more than one computer simultaneously unless the license agreement specifically allows this;
- For a staff member or any section of the University to consciously encourage or request any staff member to make, use or distribute illegal software copies;
- To infringe the laws against unauthorized software copying because a superior, colleague or friend requests or compels it;
- To loan software so that a copy can be made, or to copy software while it is on loan.
- To copy music and video and distribute to others.

NETWORK INTEGRITY

The campus computer network is recognized as a key element of the electronic based services that support the academic programs. Personal devices can be connected to the network only in accordance with the University's telecommunications standards. Details of these standards are available from Technology Services. Systems must be registered with technology services and will be allocated an appropriate network address that is compatible with the campus network. Restricted access may be enforced on personal devices. Any unauthorized form of experimentation with the campus network is prohibited.

E-MAIL

Services for electronic communications (such as electronic mail, bulletin boards, list servers and news) are provided for general use consistent with this and other University policies. Clients are responsible for the use of their account and the electronic messages, which are sent from their account. It is the responsibility of anyone issued LCU account credentials to familiarize themselves with the University's policies, regulations and procedures associated with the use of electronic communications.

Unless you specifically encrypt your personal electronic mail it is sent in clear text and is readable by anyone who can intercept the mail. It is advisable not to send confidential information that you do not wish to become public knowledge. Also, any electronic mail that is incorrectly addressed may be received by a third person or may be bounced to a "Postmaster" in an external organization for redirection.

MALWARE

Clients need to consider all of the possible points of entry (Internet, e-mail, external media, personal computers, gateways, servers, etc.) when addressing the potential risks and implement appropriate actions

to counter the risks. The success of these actions depends on the malware detection products used as well as the regular use of these products by clients. As a consequence, it is imperative that you adopt a malware protection strategy and rigorously adhere to it.

GUIDELINES FOR MALWARE

The following guidelines are provided to assist you in implementing a successful malware protection and detection strategy. Remember it is easy to introduce malware onto your computer. Electronic mail messages and Internet file transfers may contain files that could carry malware. Use caution in opening email.

If your computer is infected or you suspect that your computer may be infected by malware, contact Technology Services (see Appendix A for details) immediately so that measures can be taken to remove the malware and identify any other affected computers and storage.

Remember, always save attachments to disk and scan before executing them or opening them.

If in any doubt, contact the Technology Services for assistance. See Appendix A below.

MANAGEMENT OF SERVICES

LCU Technology Services accepts responsibility for the maintenance of University technology resources to standards of reasonable reliability and security, and for the delivery of instructional materials and training courses to enable all clients to use these resources efficiently. Support services are provided to maintain service availability and to ensure that these resources are used effectively to support the university mission and vision. Student technology resources are maintained to ensure the needs of the academic mission are met. Technology services strives to maintain the highest standards of ethical and thoughtful stewardship of university funds in the application of technology resources. This standard is the overriding principle to determine essential use, standards of performance and implementation of operational measures for technology resources.

EXPRESSION OF PERSONAL VIEWS

Correspondence, discussions and comments made by clients using the University Technology Resources may be interpreted as representative of the University's position. Personal opinion, comments and correspondence must clearly state that the opinion expressed is that of the writer, and not necessarily that of the University, or words to that effect.

OFFICIAL REPRESENTATION OF THE UNIVERSITY

Where the client is representing the views of the University, then a notation must be appended to the communication identifying the individual and the position title held within the University.

RESPONSIBILITY WITH REGARD TO LAWS, LUBBOCK CHRISTIAN UNIVERSITY POLICIES AND CONTRACTS BETWEEN THE UNIVERSITY AND EXTERNAL AGENCIES

The University has obligations relating to intellectual property, sexual harassment, and racial discrimination as defined by law, and in its own policies. The University expects all employees to act within any federal, state, or local laws. Technology Resources users will also exercise responsibilities in this area. Clients should familiarize themselves with University policies and documentation on the following matters that include but are not limited to:

1. Acceptable Use of Technology Resources
2. Faculty Handbook
3. Employee Handbook

4. All special policies located on the LCU Policies and Procedures portal.

Clients must not act fraudulently in any way, for example, making false representations about any matter, or about the authorship of any document or work, or falsely attributing the source of any material to another person, or forging anything.

LCU Technology Services has certain contractual obligations relating to the use of its technology resources, which constrain the way services, may be used. LCU may take disciplinary action against anyone whose use of services violates the terms of such agreements.

DEFAMATION, HARASSMENT AND OTHER ABUSIVE BEHAVIOR

No client will, under any circumstances take any action, which would or might lead to the University's Technology Resources being used for the purpose of defaming or slandering any individual or organization or use the system in any way such that a reasonable individual may consider it to be harassing, abusive or obscene behavior.

ILLICIT MATERIAL

No client will, under any circumstances use the University's Technology Resources to access, transfer, or store illicit material. Illicit material would include, but is not limited to, material that is threatening, obscene, discriminating, harassing, offensive, or conflicting in any way with the values of Lubbock Christian University.

CANCELLATION OF LCU TECHNOLOGY RESOURCE ACCESS

Unless otherwise stated, student technology resource access will be cancelled at the conclusion of the current period of enrollment. Staff technology resources access will be cancelled once their employment at the University terminates or the resource is no longer required to perform their duties.

Upon request by the departing employee, the Human Resources and Technology Services departments may agree to allow a departing employee continued access to LCU Technology Services so long as the departing employee's supervisor approves the continued access. The period of continued access shall be for the amount of time and for the purpose agreed to by the Human Resources and Technology Services departments and not for any longer period of time. If any one of the departments listed above fails to approve a departing employee's request for continued access to the university's technology systems, then the departing employee's access will cease at a point in time determined by the Human Resources and Technology Services departments

Clients may have their technology resources access terminated or suspended for breach of any of the terms of this policy or related policies, as determined by the person responsible for the client and the Director of Technology.

VIOLATIONS

If any client becomes aware of any action by another individual or group, which could be considered to breach this policy, they are requested to take appropriate action to ensure it is brought to the attention of LCU Technology Services and/or LCU Administrators (Appendix A).

Depending on the nature of the events, violations may be dealt with as described in the Lubbock Christian University Student Handbook and/or the Lubbock Christian University Faculty / Staff Handbook, any relevant contracts, and possibly by the law.

In most cases, the first action Technology Services staff will take to confirm the violation of University policy will be to restrict client access to Technology Resources. The client is required to contact Technology Services through the TS help desk to arrange an interview with the Vice President for Technological Advancement and the appropriate Dean(s) or Vice President(s).

A Vice President, dean or head of department, in your department or school/college will be informed of the circumstances of your case as well as any additional information arising during your interview. It is the responsibility of schools/colleges or departments to impose appropriate disciplinary actions.

Contact for Interpretation: Vice President for Technology Advancement

Appendix A

Technology Services/Chap Desk
806-720-7100 or chapdesk@lcu.edu

Vice President for Technology Advancement
806-720-7122 or karl.mahan@lcu.edu

This policy and procedure supersedes all prior policy statements on this subject.