COMPUTER USE POLICY & PROCEDURES

For Luna Community College

Table of Contents

Section - 1 Statement of Policy

Section - 2 Policy for Acceptable Use of the Internet and Campus Networks

Section - 3 Computer and Information Services Policies and Procedures

- Hardware & Software Acquisition
- LCC Standards
- Technical Support

Section - 4 Confidentiality Agreements

Section - 5 Support Forms

Section – 1

Statement of Policy

For Students and Employees

Statement of Policy

Purpose:

The purposes of these policies and procedures are to encourage computer use at Luna Community College (LCC) and to regulate computer use as necessary to protect individual privacy, to provide an equitable sharing of limited resources, to maintain standardization with the college assets, and to promote responsibility in the use of the College's computer system.

Policy:

The Luna Community College Computer and Information Services Department (CISD) provides computer services to faculty, staff and students as well as a limited number of outside clients of LCC. All computer users have two basic rights – privacy and a fair share of the resources.

All computer users have the responsibility to use the LCC computer systems in a respectful, efficient, ethical and lawful manner. The ethical and legal standards that are to be maintained are derived directly from standards of common sense and common decency that apply to the use of any public resources within the College.

LCC's policy for use of its computing facilities is based on the United States Copyright Law and the laws of the State of New Mexico Computer Crimes Act: Sections 30-45-1 to 30-45-7, New Mexico Statutes Annotated (1978). This policy incorporates the definitions in law, provides guidelines for appropriate use of computers and outlines the administrative procedures that will be imposed on any computer users who fail to comply with policy.

The following policies, rules and conditions apply to all users of LCC computer services. Violations of any of these conditions are considered a violation of LCC policy and will be treated as such. LCC views the use of computer facilities as a privilege – not a right- and seeks to protect legitimate computer users by imposing sanctions on those who abuse the privilege. Eliminating computer abuse provides more computing resources for users with legitimate computing needs.

Sanctions:

In accordance with established College practices, violations may result in disciplinary action, which could lead to expulsion from the College, temporary or permanent loss of computer privileges, or dismissal from a position and/or legal action. All computer users have a right to appeal any disciplinary action through established procedures.

The following provisions, which apply to all use of computer and network interconnections owned or administered by LCC, including campus-wide computer facilities, govern computer users.

Computer users shall:

- Respect the intended use of accounts established for their use;
- Respect the integrity of the College computer systems and networks;
- Respect the privacy of other computer users;
- Respect the rules and regulations governing the use of facilities and equipment;
- Respect the proprietary rights of software owners and comply with all copyright laws.

The Director of Computer and Information Services shall administer these policies and procedures, with oversight by the Office of the President. The policies will be reviewed at least every two years and modified and approved as necessary.

Section – 2

Policy for Acceptance Use of the Internet and Campus Network

For Students and Employees

Policy for Acceptable Use of the Internet and Campus Networks

1. **Computer users shall respect the intended use of user accounts established for their use.**

The departments, divisions, and other authorized units of LCC give authorization for the use of accounts for specific academic, administrative or other authorized institute purposes.

Computer accounts are the property of Luna Community College and are to be used only for College related work. The contents of College accounts shall be the property of the authorized user, subject to applicable College copyright, intellectual property policies, and applicable federal and state laws. If staff feel that the integrity of the system is threatened, access by Computer and Information Services Department (CISD) staff to information within these accounts may be granted by the Director of Computer & Information Services, or designee.

In other cases, authorization for non-authorized user access shall be sought from the Vice President to whom the account user reports. The respective Vice President shall notify the account user in writing. If the user is a student currently enrolled, the student's instructor should also be notified.

Prohibited are attempts to:

- Defeat the security systems of any LCC computer
- Circumvent the account system
- Use an account without authorization, or
- Use accounts for other than their intended purposes.

Use of an account which invades the rights of privacy or which misappropriates the data or files of others may subject the wrongdoer to both criminal and civil liability. LCC reserves the right to bar a computer user from a College account if the designated LCC officials determine impropriety.

LCC reserves the right to limit a computer user's session if there are insufficient resources or if the user is determined by the designated authorities to be acting in an irresponsible or unlawful manner. LCC also reserves the right to cancel, restart or place on hold a job, process or program to protect or to improve system performance if necessary.

1. **Computer users shall respect the integrity of the system.**

Computer users shall not intentionally develop or use programs or engage in behaviors that harass other computer users, infiltrate the system or damage the software or hardware components of the system. Uses of the network to access or process pornographic material, inappropriate text files, illegal activities, or files dangerous to the integrity of the network are prohibited.

Computer uses shall use great care to ensure that they do not use programs or utilities that interfere with other computer users, infiltrate the system, modify the system, modify an account or damage computer data. This includes all network connections.

Network connections shall be used only as permitted in network guidelines (e.g., INTERNET, BITNET). The use of any unauthorized or destructive program or access may result in legal civil, and/or criminal action for damages by any injured party, including the College.

LCC acknowledges the value of academic program development, research on computer security, and the investigation of self-replicating code (VIRUS). However, LCC and each computer user has the responsibility to use each of the computers systems, which are public property, in a manner related to the educational process for which they are intended. Individuals who wish to use LCC computer facilities for these purposes must plan and consult with CISD. Limitations may be imposed on these activities minimizing the effects. Restrictions on computer

security and self-replicating code are defined in a manner that protects the college and individual computing environments, but does restrict or limit legitimate academic pursuits.
The value of all computer usage depends on the availability and integrity of the system. Any defects discovered in system accounting or system security is to immediately report to The Computer and Information Services Department, so that steps can be taken to investigate and resolve the problem. The cooperation of all users is needed to ensure prompt action.

The integrity of the system is maintained by password protection of accounts. A computer user who has been authorized to use an account may be subject to both civil and criminal liability if the user discloses the password or makes the account available to unauthorized persons without permission.

Use of electronic communication utilities (such as e-mail, chat rooms, and CARS MAIL) to transmit fraudulent, harassing, obscene, indecent, profane, intimidating, or other unlawful messages is prohibited by state and federal law. Loading, or intentional receipt of hate mail harassment, and other antisocial behaviors are prohibited on the network. Also, the electronic communications facilities are not to be used for the transmission of commercial or personal advertisements, solicitations, promotions, and destructive programs or for any other unauthorized use.

1. **Computer users shall respect the privacy of other computer users**

Computer users shall not intentionally seek, provide, modify information in, gain access to accounts or obtain copies of files, programs, or passwords belonging to other computer users without the permission of those other computer users. This includes all system files and accounts.

The LCC system provides mechanisms for the protection of private information from examination by others. Attempts to circumvent these mechanism in order to gain unauthorized access to the system and/or to private information are unlawful and will be treated as a violation of LCC policy. Searching through non-public directories, libraries or any other storage media to find unauthorized information is also a violation.

Computer user, when requested in writing, shall cooperate with system administrators in investigation of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files. LCC recognizes that files and mail messages are confidential; however, authorized LCC employees may access computer users' files at any time during system maintenance and report suspected unlawful or improper activities through the proper channels.

1. **Computer users shall respect the rules and regulations governing the use of facilities and equipment.**

LCC departments and divisions may have specific rules and regulations that govern the use of computer data, equipment and facilities. They may have operators, consultants, and/or supervisors who are given the responsibility to supervise and manage access to department and division computer data and resources. The user's cooperation with these individuals and adherence to LCC policies are expected at all times. Students are encouraged to utilize the support services of CISD or lab staff; however, obtaining program code from the Labs, CISD or other staff, when forbidden by an instructor, is prohibited.

Reasonable personal use shall be allowed, provided such use does not interfere with academic use. All such improper uses cannot be anticipated or listed here, but examples may be:

- Playing computer games, when such use would interfere with the availability of facilities for academic use;
- Commercial activities or advertising;
- Libelous statements that would damage a person;
- Dissemination of licensed software;
- Invasion or violation of personal privacy; or
- WWW personal home pages which could reasonably be misconstrued to be official representations of the Community College. Use of official LCC logos on such pages, without express written consent of the college, is prohibited. LCC cannot accept responsibility for personal home page content.

1. **Computer users shall respect the proprietary rights of software.**

All software protected by copyright shall not be copied except as specifically stipulated by the owner of the copyright, or the original software is clearly identified as “shareware” or in the public domain. Protected software is not to be copied into, from, or by any LCC facility or system, expecting by license. This means that such computer and microcomputer software may only be copied in order to create backup copies, if so licensed. The number of copies and distribution of the copies may not be done in such a way that number of simultaneous users in a department exceeds the number of original copies purchased unless otherwise stipulated in the purchase contract.

Attributions of authorship will follow the copyright rules for material obtained via the network. Users will not install software on the network or individual computers; only the network administrator can authorize installation of software.

Section – 3
Computer & Information Services Policies and Procedures
For Employees Only

Computer & Information Services Policies and Procedures

The Computer and Information Services Department (CISD) was classified as an internal service to the College in the 1996-1997 fiscal year. This requires that the department be self-sufficient in its means of operation within the Institute. This organization provides critical guidelines in determining the architecture of LCC's integrated network:

- Luna Community College will maintain one network;
- The network will be centrally managed and maintained;
- And the network will be self-supporting cost center.

This policy is based on using good business practices, and following the guidelines of the LCC *Information Technology Plan* by:

- Realizing substantial fiscal and technical benefits, and
- By centralizing some purchasing and networking services, and
- By following the set standards for desktop hardware, software, and network hardware.

Luna Community College has accepted State implementation strategies for standardization of desktop hardware and personal productivity software. These standards are intended to simplify the purchasing decisions, and to lower maintenance/support costs. All services that the CISD performs are billed to the classification of "Computer Services."

In order to comply with College accepted standards, and to ensure full utilization of LCC's assets. All computer workstation equipment, devices, and software will be requested through the Computer and Information Services Department (CISD).

Personal Computer/Workstation Acquisitions

All computer equipment will be requested through the Computer and Information Services Department (CISD). Individual department directors will submit the request through CISD buyer by identifying the following:

1. Describe the use and intention of the equipment being requested,
2. Identify the primary user for the requested equipment.
3. Identify if this item is a new workstation, replacement for outdated equipment, or an upgrade/enhancement for an existing workstation. If this item is a replacement, please include a description of what will become of the replaced equipment or if it will be available for use/disposal at the CISD discretion.
4. Provide the estimated time of implementation by your department. This may not coincide with the CISD scheduled activities, but will provide CISD with scheduling information.
5. Provide the quantity of items that you are requesting.
6. Provide the location (i.e. office room number, classroom number) that the equipment will be located.

Computer workstations and printers will be scheduled for installation once the item has been received and processed by the Shipping and Receiving Department. Scheduling will be based on the current workload of the CISD Department. There may be other factors (internal and external) that will delay the processing of the requested order once the CISD Department has processed the initial requisition. CISD will contact the Department Director when the supplying vendor has received the order, and when the vendor has supplied an estimated time of arrival at our campus.

Items that may be needed to complete the intended request will be discussed with the Department Director once the request has been reviewed and preliminary contact has been made with the supplier. Software costs may need to be included at the time of review and may impact the amount needed to implement the equipment. If software is not included at the time of the equipment order, the workstation may not be operational as per planned intentions. *See policy on "Software Acquisitions" for details on ordering software packages.*

Computer hardware options must also be included in your equipment requests. *See policy on "Personal Computer/Workstation Acquisitions" for details on ordering computer software.*

Printer Acquisitions.

All printer equipment will be requested through the Computer and Information Services Department (CISD). Individual department directors will submit the request through CISD buyer by identifying the following

1. Describe the use and intention of the equipment being requested,
2. Identify the primary user for the requested equipment.
3. Identify if this item is a new printer, replacement for outdated equipment. If this item is a replacement, please include a description of what will become of the replaced equipment or if it will be available for use/disposal at the CISD discretion.
4. Provide the estimated time of implementation by your department. This may not coincide with the CISD scheduled activities, but will provide CISD with scheduling information.
5. Provide the quantity of items that you are requesting.
6. Provide the location (i.e. office room number, classroom number) that the equipment will be located.

Printers will be scheduled for installation once the item has been received and processed by the Shipping and Receiving Department. Scheduling will be based on the current workload of the Computer Services Department. There may be other factors (internal and external) that will delay the processing of the requested order once the CISD Department has processed the initial requisition. CISD will contact the Department Director when the supply vendor has received the order, and when the vendor has supplied an estimated time of arrival at our campus.

Software Acquisitions

All computer software will be requested through the Computer and Information Services Department. Department Directors will submit the request through the Computer Services Department by identifying the following:

1 Describe the use and intention of the software being requested.
2. Identify the primary user and computer workstation accessing the requested software. Include computer identification name if possible.
3. Provide the estimated time of implementation by your department. This may not coincide with the CISD scheduled activities, but will provide the CISD with scheduling information.
4. Number of copies (user licenses) of workstation software that you are requesting.
5. The location (i.e. office room number, classroom number) that the software will be installed,

Software will be scheduled for installation once the media has been received and processed by the Shipping and Receiving Department. Scheduling will be based on the current workload of the Computer Services Department. There may be other factors (internal and external) that will delay the processing of the requested order once the CISD Department has processed the initial requisition. The computer Services Department will contact the Department Director once the supplying vendor has supplied an estimated time of arrival at our location.

Items that may be needed to complete the intended request will be discussed with the Department Director once the request has been reviewed and preliminary contact has been made with the supplier. Hardware upgrade costs may need to be included at the time of review and may impact the amount needed to implement the software. If hardware upgrades are not included at the time of the software order, the workstation may not be operational as per planned intentions. At the time of the review, CISD may determine if one of the LCC standard software licenses currently in place may cover the intended request.

* Technical Support

Personal Computer Technical Support Procedures

Service Requests.

Computer Service Work orders (Repair Work Orders)

The work order request gives the CISD a mechanism for scheduling and tracking service order requests. Work Order Request should be in an email request to support@luna.edu.

Any service call that requires the CISD staff to perform an on-site visit to assist with problems associated with hardware, telecommunications, or software must be accompanied by a "Support Ticket" before the assigned task can be completed. Users must be aware that their request may not be the only order pending. To ensure that supervisors are aware of changes or specific problems within their departments, a supervisor or director must be Carbon Copied (Cc) on all "Work order Request". Technical assistance will be available by telephone when at all possible and must be followed up by a "Work Order Request".

1. Information that is needed by the technician is as follows:
   - Employee filing the request
   - Date the employee is completing the form
   - Location with building and room number of the machine or problem
   - The LCC Machine ID number (or tag number)
   - Clear, concise description of the problem.

   Employees are encouraged to determine to the best of their ability if the problem is CPU related, printer related, or monitor related.

2. Employee will also need to describe in as much as possible, the problem that they are encountering, the steps that they have taken to correct the problem before the request was issued, and any other related details that will assist the technician.
3. CISD will date stamp all work order requests when received and will schedule the request based on current priorities and importance of the problem encountered. Some repairs may require longer time to resolve. Repairs may require parts to be ordered, which will add to the amount of time needed to complete the repairs.
4. Emergency calls will be handled immediately if the need is determined at the time of the problem. CISD will make arrangements for a substitution of equipment (if available) when an emergency call requires a piece of equipment to be replaced. The replacement or repair of the damaged equipment will be ordered as soon as possible. If the item is required to be sent to an outside facility, CISD will process the needed request.
5. If a service call is performed and it is determined that the problem is related to an installation of a non-authorized software package or hardware item, Administration and the responsible Department Director will be notified of the incident that was encountered and the circumstances involved. Any action taken concerning the incident will be determined by the sanctions in the *Statement of Policy.*
6. Non-emergency calls will be scheduled during the afternoon hours of operation. If the call has to be escalated to a higher priority, the call will be scheduled during the morning hours. Major software installations may require more time for installations and will be scheduled accordingly. Problems encountered within instructional labs will be handled during non-scheduled times if at all possible. When not possible, students may have to be relocated to a working station when repairs take place.

Problems that are encountered within an instructional lab or student use area will take priority over non-instructional areas and staff offices. Network problems will be of high priority due to the fact that these problems affect the greater amount of people at one given time. Problems that affect the integrity of date recorded by the College will be given the highest priority. Problems with the network communications will be the responsibility of the CISD Department.

Computer and Information Services Technical Support Responsibility.

1 The CISD technical staff will perform maintenance on all the computer equipment that was purchased by the College for use within the departments. If the equipment carries a required service agreement with an external service organization, the CISD staff will assist when the need requires and with the approval of the organization that is providing the service contract on that equipment. If the equipment is provided to the College by another agency organization, at the time of the service request, a review will be done to determine the correct procedures for handling the repair. This review will consist of who is responsible for any cost associated with the labor and repairs.
2 The CISD will be responsible for ordering all replacement computer equipment and supplies necessary to complete the repair order request.
3 The CISD staff will be responsible for reporting on a regular basis to the office of the President. These reports will consist of reviews of (work orders) service calls, repairs, and installations.
4 If CISD is performing frequent repairs within the same area, review and recommendations will be presented to both the department and the Director of Fiscal Operations for input on resolving the frequent service calls.

Computer Services Planning.

1 As stated above, the CISD staff will need to schedule the repair or service call. Proper planning is necessary by the department requesting the service or the wait may have an impact on the delivery of instruction to students, or delay administrative services to the College. Depending on when the CISD receives the request, the issuing department may not have the equipment available by the time that they require. The time needed to complete the repair may not be within the time frame that the issuing department required; this depends on the amount of time required to resolve the problem, once it is located.
2 Minor repair requests need to be submitted at least 4 hours prior to scheduling the repair. This still may impact on currently scheduled repairs, so requestors must be aware the request will be scheduled as soon as possible.
3 Major repair requests will require 4 to 5 working days prior to repair. This may also impact the currently scheduled repairs, but will be scheduled as soon as possible. Some delays may be experienced if replacement parts will need to be ordered.
4 Major software installs and re-installs for computer laboratories will be scheduled during semester breaks to allow full access to the labs. A list of needed software for each lab must be requested one semester in advanced. This will allow the software to be scheduled for correct installation and testing prior to start of classes. New software must be ordered and received before scheduling can take place.

Moving of College Computer Equipment and Software.

1 Any transfer of equipment is subject to approved requests for transfers from the Warehouse. If this transfer is computer related, copies of the transfer must be sent to the CISD.
2 The CISD will maintain separate records as to the location of computer related equipment. This will include details on what is included in the equipment that has importance to CISD for future planning.

3 Software transfers will be recorded by CISD to assist with requirements pertaining to software licenses. Departments will inform CISD about requests to transfer software licenses. All College software license documentation will be housed in the CISD vault.

Computer systems accounts and passwords.

It is the responsibility of the user to observe good security practices. Irresponsibility by the user causes security failures and allows the College's computer systems to become vulnerable to unauthorized access. Employees working with student data are to sign and submit to their supervisor/director an Acceptance of System Password(s) form, and an Agreement of Security and Confidentiality (shown in sections 4).

The network operating systems in place by the College provide basic mechanisms to allow control of the systems and data. To help ensure a safe and secure computing environment the user should be cognizant of the following information.

Password protection is used to restrict unauthorized access to the computer systems. Users play a large role in helping to reduce the potential for password detection.

Accounts for the network users require a Username and Password. The initial password allows users to logon to the system but they are required to change their passwords during the first login.

The network is the primary logon that the College staff uses to access the network systems. The CARS Information System has a separate Username and Password. Instructional laboratories use the Microsoft operating system for logging on the lab workstations. Instructional lab system is separate from the network and CARS Information System. E-mail passwords are assigned when the account is requested by the department director/supervisor and enabled.

Passwords are required to be a minimum of 6 characters long, when constructing passwords do not use obvious patterns, or any associations with the user. (i.e. Birth Date, Spouses, Children, or favorite per names).

Passwords should be changed regularly or when you suspect someone may know your password. The individual users should change e-mail and CARS passwords regularly. Whenever CISD Staff changes a user's passwords on any of the network systems, the user should change the password once the user signs on to that system.

Users should never leave a terminal unattended that they have logged onto the system with. Users will be held responsible for any actions taken by their Username. (See policy for Acceptable Use of the Internet and Campus Network). Refrain from sharing your password with others. Avoid multiple-user access to the same account unless it is setup for this purpose. Refrain from writing passwords down and placing in an unsecured location.

Report any problems gaining access to the system with a Username/Password combination that you believe should work. Users are responsible for their account and data. Access is granted to individuals for their use. Misrepresentation, misuse and carelessness may result in lost data or system privileges. Forgotten passwords or failure to change passwords within the given grace period will be logged and reported to Department Directors and Administration. Unattended workstations or unauthorized access of a user's account and password will also be reported. This is in accordance to the procedures required of the CISD Department in regards to "Security Issues and Violations."

Requests for Network and E-mail accounts and passwords should be directed to the Computer and Information Services Department staff at extension 1070. CARS Information System accounts and passwords should be directed to the Information Systems staff at extension 1161. Department directors must use the Employee Technology Account Request form (in section 5).

Section - 4
Confidentiality Agreements

- Agreement of Security and Confidentiality
- Acceptance of System Password(s)
- Email Acceptable Use Policy

Luna Community College
Office of Computing and Information Services
and the Office of Human Resources

2020-2021 Academic/Fiscal Year

Agreement of Security & Confidentiality

Security and confidentiality of all College records and student education records is a matter of concern for all employees who have access to files or the computerized databases owned by the College. The databases are a repository of computerized information stored in the computer systems of the College and maintained by the owners. It is the express understanding of Luna Community College that the Student Education Records through access will be employed only by school officials who have a legitimate interest, and for the purpose from which it was requested and will not be released to any other individual or office for another purpose. A school official has legitimate interest if the official needs to review an education record in order to fulfill his/her professional responsibility. A person having access to student records should be aware that there are possible civil sanctions and LCC disciplinary action for violating records privacy agreements.

Each person working with the system holds a position of trust and must recognize the responsibility of preserving the security and confidentiality of the information. Since a person's conduct either on or off the job may threaten the security and confidentiality of the information, any employee or person with authorized access to the system is expected:

1. To keep personal passwords private. Passwords are not to be written or shared with others. Individuals who do not have access must contact Computing and Information Services to secure that access.
2. To always log off of computer when leaving the immediate area.
3. Not to allow any operator to use computer which has been signed on under any other operator's user ID and password.
4. Not to permit unauthorized use of any information in the files.
5. Not to seek personal benefit or permit others to benefit personally by any confidential information which has come to them through their work assignment.
6. Not to exhibit or divulge the contents of any record or report to any person except in the conduct of their regular work assignment.
7. Not to include knowingly or cause to be included in any record or report a false, inaccurate, or misleading entry.
8. Not to remove any official record or report (or copy) from the office where it is kept except in performance of regular duties or in cases with prior approval.
9. Not to operate or request others to operate any College data equipment for purely personal business.
10. Not to aid, abet, or act in conspiracy with any other person to violate any part of this code.
11. To report any violation of this code to the supervisor immediately.

I understand my acceptance of access to College Records, Student Records, and Schedule of Classes within the College Information System signifies I accept the responsibility for complying with the College policy for the release of Information. I have read this Agreement of Understanding and the explanation of access guidelines. By my signature below, I understand and agree to comply with these provisions, and to preserve the security and confidentiality of information I access. Failure to comply may lead to suspension or dismissal consistent with the general policies of the College.

Employee Name (printed or typed) _____

Signed _____ Date_____

This form is to be maintained for all employees and kept on file by the Office of Human Resources. (06/11)

This page intentionally left blank.

Luna Community College
Office of Computing and Information Services
and the Office of Human Resources

2020-2021 Academic/Fiscal Year

Acceptance of System Password(s)

Passwords are used to protect Luna Community College information resources that contain information critical to the operation of the College and to protect sensitive data. The use of a password assures access by authorized personnel only when passwords are kept secret. Therefore, the password(s) issued to you should be protected as follows:

1. Never give a password to another person, even an LCC employee.
2. Passwords are not to be written or shared with others.
3. For disposal, any piece of paper on which a password has been written must be torn up or shredded.
4. When a password has expired, a new password must be changed as soon as notification has been given. Failure to change password may cause you to be locked out of system until your password can be reset.
5. Passwords should not be the same as the user ID, should not be a person's name, a single common word, a birth date, or part of a social security number or employee id number. The best type of password has six or more, both alpha and numeric characters in logical order or sequence.
6. Always log off at a password-protected computer when it will be left unattended.
7. Use your password-granted access for authorized updates only.

An authorized update is one that is required for you to complete your assigned task within the computer system that you are using.

The network password that you have been issued will expire at the time of your first login, or at the time of a password reset. You must change your Jenzabar password periodically at your discretion.

Failure to comply with these requirements may be grounds for Administrative action.

I have read and understand my responsibilities to protect the information resources that I will use in the performance of my job.

Employee Name (printed or typed) _____

Signed _____ Date _____

This form is to be maintained for all employees and kept on file by the Office of Human Resources. (06/11)

This page intentionally left blank.

Luna Community College
Office of Computing and Information Services
and the Office of Human Resources

2020-2021 Academic/Fiscal Year

E-Mail Acceptable Use Policy

E-mail is a critical mechanism for business communications at Luna Community College. However, use of Luna Community College's electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of Luna Community College.

The objectives of this policy are to outline appropriate and inappropriate use of Luna Community College's e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

Scope

This policy applies to all e-mail systems and services owned by Luna Community College, all e-mail account users/holders at Luna Community College (both temporary and permanent), and all company e-mail records.

Account Activation/Termination

E-mail access at Luna Community College is controlled through individual accounts and passwords. Each user of Luna Community College's e-mail system is required to read and sign a copy of this E-Mail Acceptable Use Policy prior to receiving an e-mail access account and password. It is the responsibility of the employee to protect the confidentiality of their account and password information.

All employees of Luna Community College maybe provided an e-mail account. Applications for these accounts must be submitted in writing to Computing and Information Services. All terms, conditions, and restrictions governing e-mail use must be in a written and signed agreement.

E-mail access will be terminated when the employee terminates their association with Luna Community College, unless other arrangements are made. Luna Community College is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

General Expectations of End Users

Important official communications are often delivered via e-mail. As a result, employees of Luna Community College with e-mail accounts are expected to check their e-mail in a consistent and timely manner so that they are aware of important company announcements and updates, as well as for fulfilling business- and role-oriented tasks.

E-mail users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to remove himself or her from the list, and is responsible for doing so in the event that their current e-mail address changes.

E-mail users are also expected to comply with normal standards of professional and personal courtesy and conduct.

Appropriate Use

Individuals at Luna Community College are encouraged to use e-mail to further the goals and objectives of Luna Community College. The types of activities that are encouraged include:

- Communicating with fellow employees, business partners of Luna Community College, and clients within the context of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities. **Inappropriate Use**

Luna Community College's e-mail systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual e-mail use will not interfere with others' use and enjoyment of Luna Community College's email system and services. E-mail use at Luna Community College will comply with all applicable laws, all College policies, and all College contracts.

The following activities are deemed inappropriate uses of Luna Community College systems and services and are prohibited:

- Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, sexual harassment, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Use of e-mail in any way that violates Luna Community College's policies, rules, or administrative orders.
- Viewing, copying, altering, or deletion of e-mail accounts or files belonging to Luna Community College or another individual without authorized permission.
- Sending of unreasonably large e-mail attachments (sending files). The total size of an individual e-mail message sent (including attachment) should be 2 MB's or less.
- Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.
- Excessive personal use of Luna Community College e-mail resources. Luna Community College allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. Luna Community College prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-College commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

Monitoring and Confidentiality

The e-mail systems and services used at Luna Community College are owned by the College, and are therefore its property. This gives Luna Community College the right to monitor any and all e-mail traffic passing through its e-mail system. While the company does not actively read end-user e-mail, e-mail messages may be inadvertently read by IT staff during the normal course of managing the e-mail system.

In addition, backup copies of e-mail messages may exist, despite end-user deletion, in compliance with Luna Community College's records retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss.

If Luna Community College discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify an employee if his or her e-mail records are to be reviewed. Notification may not be possible, however, if the employee cannot be contacted, as in the case of employee absence due to vacation.

Use extreme caution when communicating confidential or sensitive information via email. Keep in mind that all e-mail messages sent outside of the College become the property of the receiver. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply" command during e-mail correspondence.

Reporting Misuse

Any allegations of misuse should be promptly reported to the Computing and Information Services, Network Operations and System Administrator at extension 1207. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the individual named above.

Disclaimer

Luna Community College assumes no liability for direct and/or indirect damages arising from the user's use of Luna Community College's e-mail system and services. Users are solely responsible for the content they disseminate. Luna Community College is not responsible for any third-party claim, demand, or damage arising out of use the Luna Community College's e-mail systems or services.

Failure to Comply

Violations of this policy will be treated like other allegations of wrongdoing at Luna Community College. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use on Luna Community College's e-mail systems and services may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of e-mail access;
2. Disciplinary action according to applicable Luna Community College policies;
3. Termination of employment; and/or
4. Legal action according to applicable laws and contractual agreements.

E-Mail User Agreement

I have read and understand the E-Mail Acceptable Use Policy. I understand if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or college policy.

Name: _____

Signature: _____

Date: _____

This form is to be maintained for all employees and kept on file by the Office of Human Resources. (06/11)

This page intentionally left blank.

Section - 5
Support Forms

- Employee Technology Account Request
- LCC Computer Usage Acknowledgement Form

This page intentionally left blank.

Luna Community College

Computer Information Services Department

Employee Technology Systems account request

Today's Date: _____

EMPLOYEE INQUIRY INFORMATION

Employees Full Name:		Employee #:	
Job Title:		Assigned Dept.:	
Prior LCC e-mail address:		Phone/Extension:	
Office Location (Building & Rm #)		Supervisor/Director Signature:	

INQUIRY DETAILS

Type of Account Requested: (Check all that apply)

Telephone Support:	
Needs Phone	☐
Voice Mailbox Reset/Setup	☐
Long Distance Code	☐
PC Network Account	☐
☐ ***Student/Employee need account access***	
CARS Account (with completed training)	☐

Start/Hire Date: _____

This Employee is: ☐ New Hire ☐ Current Employee
☐ Transferred Position
☐ Re-Hire (Had previous accounts)

Approval to add new accounts listed above:

Date: _____ Human Resources: _____

I.T. Office use only

Account	Date Enabled	Entered by	Notes: (module, account name)
Voice Mailbox			
Long Distance			
Network			
E-Mail			
CARS Account			

This page intentionally left blank.

LCC COMPUTER USAGE ACKNOWLEDGEMENT FORM

I, _____, acknowledge that the Human Resources Department has given me the Luna Community College Computer Use Policy and Procedures handbook adopted on August 11, 2015. I am also aware it is available on the LCC website under the Information Technologies Tab. I acknowledge that I understand policies and procedures within this manual.

I also acknowledge that during review/discussion, I was given the opportunity to discuss policies and ask questions.

_____
Signature

_____
Date

This form is to be maintained for all employees and kept on file by the Office of Human Resources. (06/11)