College of Lake County

Directives on Acceptable Use of Technology Resources at College of Lake County

Version 4.0
October 2013

Table of Contents

Purpose

The technology users at the College of Lake County have access to valuable college resources, to sensitive data and, to external networks. Consequently, it is important for all users to behave in a responsible, ethical and legal manner. In general, appropriate use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. This document establishes more specific guidelines for the use of all information technology resources owned or managed by the College of Lake County including external network services, such as the Internet, which may be accessed via the college's Information Technology facilities.

Individual departments/divisions may have additional guidelines regarding information technology equipment in those departments/divisions. However, those guidelines should at least conform to these directives at the minimum. Contact the division/department chair for more information about Information Technology policies in a specific department.

By using the technology resources at the College of Lake County, it is assumed that the user agrees to abide by the policies that govern the use of the resources.

Guidelines for Appropriate Information Technology Use

The following list, while not exhaustive, provides some specific guidelines for responsible and ethical behavior when using information technology:

Use only the computers, computer accounts and computer files for which you have authorization. Do not use another individual's electronic ID or account, or attempt to capture or guess other users' passwords. Users are individually responsible for all use of resources assigned to them; therefore, sharing of accounts is prohibited.

Obey established guidelines for any computers or networks used both inside and outside the college. For example, individuals using the college's public information technology labs/classrooms must adhere to the policies established for those labs/classrooms; individuals accessing off-campus computers via external networks must abide by the policies established by the owners of those computers as well as policies governing use of those networks.

Do not attempt to access restricted portions of the network, an operating system, security software, or accounting software unless authorized by the appropriate college administrator or owner. Breaking into computers is explicitly a violation of Internet rules of conduct, no matter how weak the protection is on those computers. Tapping into telephone or network lines is a clear violation of college policy.

Abide by all state and federal laws.

Respect the privacy and personal rights of others. Do not access or copy another user's electronic mail, data, programs, or other files without permission.

Abide by all applicable copyright laws and software license agreements. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright

infringement. The unauthorized use or distribution of copyrighted works (including Web page graphics, sound files, trademarks and logos) is prohibited and may provide the basis for disciplinary action, civil litigation and criminal prosecution. Respect the copyright law as it applies to images, texts and sounds in the production of electronic information.

Use appropriate standards of civility when using information technology systems to communicate with other individuals. Using the college's information technology resources to harass other individuals deliberately is explicitly prohibited.

Be sensitive to the needs of others, and use only your fair share of information technology resources. For example, users of shared resources, such as the central computer or the public labs/classrooms, should use these facilities for only the most essential tasks during periods of peak demand. Broadcasting non-sanctioned messages to large numbers of individuals and sending chain letters are examples of activities that cause network congestion and interfere with the work of others, and thus are not allowed.

Information technology resources and electronic information are a valuable college resource. Protect your data and the systems you use. For example, back up your files regularly and follow password guidelines. Make sure you understand the access privileges you have set for your files and computer system. Do not destroy or damage any information technology equipment, networks or software. The willful introduction of computer viruses, worms, Trojan horses or any other infection into the College of Lake County Information Technology environment or into other information technology environments via the college's network violates college standards and regulations.

Use the college's information technology facilities and services for college related work. Use of college information technology resources for personal financial gain requires prior approval. Contact the Vice President for Administrative Affairs for detailed information. Activities that would jeopardize the college's tax exempt status are prohibited.

The information technology environment at the college is continually evolving as new products are introduced and others become obsolete. The Information Technology Services department will strive to keep the college community informed about these changes in a timely manner and ensure that instructional documentation and/or training is made available to those users who need it. Users are responsible for paying attention to communication sent from the ITS department and to adapt to these changes as members of the college community.

The primary use of college technology by students should be for course-related work. When labs are busy, users may be asked to limit non-course related personal tasks and/or give up their space to students doing homework and research. Computer lab users who are not affiliated with the college may be asked to move to give students and staff priority access to technology and information resources.

Data Integrity & Security

All members of the CLC community share in the responsibility of protecting any sensitive personal data they come in contact with while using technology services at the college. Sensitive data includes personal and financial information protected under the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), Children’s Online Privacy Protection Act (COPPA), Fair and Accurate

Credit Transactions Act (FACTA), **Health Insurance Portability and Accountability Act (HIPAA),** and the Payment Card Industry Data Security Standard (PCI-DSS) and all future information protected by new and updated laws and industry standards.

Breaches of certain sensitive data may subject the college to fines and/or criminal penalties and harm to its reputation. Access to this type of information is restricted and requires prior authorization from a Vice President. It is recommended that sensitive data be stored on secure servers maintained by ITS and not download locally to personal computers, smartphones, tablets, laptops, or other mobile devices unless absolutely necessary and with proper encryption, security controls, and prior approvals. Sensitive data should not be shared with third parties outside of the college in an unsecure manner, such as through unencrypted email or unsecure Web servers. Users are encouraged to log off from computers and secure mobile devices. In the event a user suspects data has been compromised as a result of device loss, theft or intrusion, ITS should be notified immediately.

ITS provides reasonable security against intrusion and damage to files stored on the central information technology services. However, neither the college, nor any ITS staff, can be held accountable for unauthorized access by other users, nor can they guarantee protection against media failure, fire, floods, etc. Users of the college's information technology resources are responsible for the backup of their files except where centralized services provide that protection.

ITS staff will assist in implementing procedures to maximize security and will provide documentation and training, as necessary, to help ensure users meet security recommendations. At a minimum, users will be required to reset their email and voicemail passwords several times throughout the year. All servers used for administrative services should be managed by ITS and stored in ITS environments.

Privacy

Members of ITS staff are forbidden to log on to a user account or to access a user's files unless the user gives explicit permission (for example, by setting file access privileges). ITS staff is also forbidden to edit any data unless it is a mass data operation that requires the technical expertise of the ITS staff and the process is initiated and monitored by the administrator in charge of the data.

Exceptions to this privacy directive are made, however, under specific conditions. One such condition is if there is a service suspected of causing disruption or using substantial bandwidth on the network or other shared services. Another condition is a suspected violation of any technology directive, or of state or federal law. In these instances, the Vice President for Administrative Affairs (or a designated agent) must be convinced that there is sufficient cause to review a file(s) before those files can be searched without the user's permission.

Before logging onto a user's account or accessing a user's private files, a reasonable attempt will be made to contact the user to inform him or her that ITS will access the files. If that is not possible, the Vice President for Administrative Affairs or an authorized agent will view the files for the suspected violation and will inform the user afterward that the files have been reviewed. Information obtained in this manner is admissible in legal proceedings, or in a college hearing. In accepting a user account, the user agrees to these terms of technology use.

Similar guidelines should be used for departmental databases or division/departments where there is a system administrator.

Network/User ID

A College of Lake County electronic ID is a unique identifier assigned to each user of campus information systems. Combined with the appropriate password, the ID can provide access to a variety of systems at the College of Lake County, including electronic mail, public computing centers, PeopleSoft, NT servers, and various web-based systems including the College of Lake County Intranet.

Password Guidelines

Why Are Strong Passwords Important?

Passwords are used to control access to College of Lake County systems, networks, applications, accounts, and data. A compromised password not only puts a user's email and files at risk, but may also expose sensitive CLC data and systems. All members of the CLC community are responsible for taking the appropriate steps to select and secure their passwords.

It is also a must to have a strong password policy in place to meet regulatory requirements and audit requirements.

This document outlines the guidelines and requirements for the choosing, managing, and protecting strong passwords at CLC.

Guidelines for Selecting Strong Passwords

One of the most common methods that attackers use to guess passwords is known as a *brute force attack*. In a brute force attack, the attacker systematically tries possible passwords until he manages to break into an account. Attackers frequently use dictionary files to generate lists of possible passwords. By choosing passwords that are easy to remember but hard for an attacker to guess, you will significantly improve the security of your computer and data.

Strong passwords have the following characteristics:

- Are at least eight characters in length
- Contain at least one alphabetic character
- Contain at least one numeric character
- Contain at least one punctuation or symbol character (e.g. !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are not trivially derived from the user's CLC Network ID, name, or a dictionary word.
- Password changes occur every 90 days.

Information service providers may set additional password requirements beyond those listed above for specific applications, systems, and services as appropriate.

When selecting passwords, keep the following guidelines in mind:

- Choose a password that is at least eight characters in length.
- Create passwords that contain all of the following: uppercase and lowercase letters, numbers, and punctuation and symbol characters (e.g. !@#$%^&*()_+|~-=\`{}[]:";'<>?).
- Avoid using dictionary words in your passwords. This includes foreign language words, slang, jargon, and proper names.
- Avoid using passwords that contain words associated with CLC, such as Lancers, Grayslake, Brandel etc.
- Avoid common misspellings and substitutions in your passwords (e.g. replacing "e" with *"3"* or *"i"* with *"1"*)
- Avoid using passwords that are based on your name, userid, birthdates, addresses, phone numbers, relatives' names, or other personal information.
- Do not use sample passwords, such as the ones included in this guide

Guidelines for Protecting Your Passwords

- All passwords are to be treated as confidential CLC information.
- You are responsible for the security of your passwords.
- Do not share your passwords with anyone, including supervisors, administrative assistants, secretaries, and technology service providers. It is against CLC policy for a technology service provider to request a user's passwords. If someone demands a password, refer him to this document or have him call the Help Desk.
- Do not use your CLC Network ID password for any other account or service at CLC or elsewhere. Your CLC Network ID password should be unique from every other password that you use.
- Avoid using the same passwords for CLC accounts as for other non- CLC access (e.g., personal ISP accounts, free online email accounts, instant messaging accounts, other online services, etc.). This will limit your exposure if any of your passwords are compromised.
- Avoid storing passwords within applications or using the "Remember Password" feature (e.g. Netscape Messenger, Internet Explorer, etc.). These features typically do not adequately protect passwords, and it may be possible for a computer virus or unauthorized user to gain access to this information.
- Do not write passwords down or store them anywhere in your office. Do not store passwords in a file on any computer system (including PDAs or similar devices) without using strong encryption.
- If you suspect your account or password has been compromised, report the incident to the Help Desk and change the password immediately.

Administrative Data Usage Directives

The Family Educational Rights and Privacy Act of 1974 (FERPA), plus its amendments, set forth rights and responsibilities regarding the privacy of student record information. FERPA governs release of student records maintained by the college and access to these records. For detailed information about FERPA contact the Director of Enrollment Services or visit the American Association of Collegiate Registrars and Admissions Officers (AACRAO) website or visit the CLC intranet Professional Development Website.

All employees of the College of Lake County (faculty, staff and student workers) are required to abide by the regulations of FERPA and those of the college regarding access to and use of student information, college financial information and college alumni information.

Department heads, division heads, directors and other supervisory personnel are responsible for ensuring that their respective employees follow the FERPA and College guidelines.

The college houses its administrative data on servers managed by ITS. Employees who have access to administrative system data must understand and accept the responsibility of working with confidential data. In addition to FERPA, college rules apply to all employees with an administrative system account.

1. Each employee is given a username and password. This account is for your use only and should not be shared with your supervisors, co-workers, family, or friends.

2. Each employee will be held responsible for any data input into or retrieval from the administrative system via their account.

3. Your administrative account is for use during those times when you are using the system for work-related activities only. Access at times other than when you are working for the college is prohibited.

4. Information that does not relate to the work assigned by your supervisor should not be viewed (e.g. looking up friends or co-workers) or altered (e.g. changing a friend's address) in any way.

5. Since administrative data is confidential, no employee will discuss or share any data they have access to with any other person on campus or off campus except as is needed to carry out their job and its responsibilities.

6. All access to electronic data and reports shall be secured. Sign off the system, put reports away in drawers and/or cabinets when leaving your work areas, especially for long periods of time. If possible lock drawers or office doors.

Acceptable Use of Voicemail

Use of the voicemail system to send fraudulent, harassing, obscene, indecent, profane, or intimidating messages is prohibited. Messages and/or materials containing such content are not to be sent from or stored on college-owned facilities.

The use of any computing resource for any commercial purpose is prohibited. This includes the transmission or relaying of unsolicited commercial email, the retailing/whole-selling of products, or the advertising by/for a profit-making entity.

Sending of unsolicited emails to large groups of users, on or off campus, is strictly prohibited. Violators of these Directives may lose their email privileges.

The voicemail system is non-confidential medium, and as such, College of Lake County's voicemail system should not be used to convey confidential or sensitive information.

The College of Lake County uses a Voice Over Internet Protocol (VOIP) phone system which is integrated into the network. As such, precautions should be made to protect the phone system in order to ensure that the network is not subsequently compromised due to intrusion. Minimally, these precautions include setting a voicemail password.

Guidelines for VoIP Voicemail Passwords:

- Voicemail passwords must be a minimum of 6 numeric characters in length
- Passwords can not be:
  - the same as the last three passwords
  - all the same digits (ex. 999999)
  - consecutive (ex. 123456)
  - contain your extension
  - spell the name of the voicemail subscriber
- Password changes will be required by the system after the password is 120 days old

Acceptable Use of Email

Email systems are a non-confidential medium, and as such, College of Lake County's email systems should not be used to convey confidential or sensitive information.

Use of the electronic communication facilities to send fraudulent, harassing, obscene, indecent, profane, or intimidating messages is prohibited. Messages and/or materials containing such content are not to be sent from or stored on college-owned facilities.

The use of any computing resource for any commercial purpose is prohibited. This includes the transmission or relaying of unsolicited commercial email, the retailing/whole-selling of products, or the advertising by/for a profit-making entity.

Sending of unsolicited emails to large groups of users, on or off campus, is strictly prohibited. Violators of these Directives may lose their email privileges.

College of Lake County electronic ID's may have associated Internet publishing capabilities (web site addresses). In such cases, use of these capabilities is subject to the College of Lake County World-Wide Web Policies, when developed.

Falsification of email headers and other intentional misrepresentation of the true sender of email items will be considered forgery and is prohibited.

All Member Distribution

"All Member" Distribution should be used for office college business only. You can post announcements on "General Announcements – CLC – Public" or "General Announcements – Non CLC" in the public folders of our email system.

Email Attachments

Emails should not have an attachment that exceeds the limit set by the college. Please call the Help Desk for current attachment size limitations.

Privacy

Notice is hereby given that although every precaution is taken to ensure privacy and security, electronic mail is not normally authenticated or encrypted. Users should not consider electronic mail to be a secure method of information transmission.

Notice is further given that certain system administrators may have access to the full content of user accounts. In no case will such administrators access such content without the permission unless instructed by campus officials as part of a legal investigation. Incidental viewing of contents may occur during certain, rare system maintenance routines. Additionally, system administrators may choose to access account contents if a perceived threat to system security is discovered. In such cases, the user will be notified as soon as possible by the administrator.

Email Use Regarding Student Record & Directory Information Notice

It is important to note that electronic mail files may be considered a student record and may be subject to all applicable federal, state, and local laws regarding such records. In general, the college will treat electronic mail in the same manner as student records in regards to day-to-day activities. Upon appropriate legal order and/or advice of counsel, electronic mail and/or associated user files may be subject to disclosure, including any records stored on backup media.

The College of Lake County Electronic ID name and the associated electronic mail address is considered directory information. Such information may be published in print or electronic format along with other directory information. Students wishing to be removed from such publications should contact the Information Technology Services Help Desk (helpdesk@clcillinois.edu).

Email Account Expiration

College of Lake County electronic email accounts are valid for the following periods:

Students – account will be deleted if extended period of non use
Adjunct Faculty/Staff - through the end of the academic year (usually around May 15th)
All other Faculty/Staff, excluding emeritus - Length of employment

If a user ceases to be associated with the college, prior to the above listed periods, a 90-day grace period will apply before the account is removed. If the association ends due to expulsion, termination of employment, or similar circumstances, the grace period may not be honored and the account may be revoked immediately.

After an account has expired, it will be permanently closed, and all files will be deleted. In no case will any additional forwarding period be granted, nor will any associated files or messages be saved or retrieved from archival tapes.

In all cases backup of personal folders, archived email on local PCs and user's data files is the responsibility of the user.

Email Filtering

The college will make use of spam filtering technology on all email accounts assigned to faculty and staff.

Liability

In no case will the college be liable for any data loss, or failure to deliver data or email due to equipment failure, unavailability of resources, or negligence.

The college backs up the network drives but not the data on the local hard drive (for example C:). The college will make every attempt to restore the data from the network drives but complete restoration might not be possible.

In all cases of liability, the user shall consider the College of Lake County to be a common carrier, exempt from liability for any content that passes through its networks.

Computer Technician Obligation Under Law

According to section 4.5 of IL law 325 ILCS 5/4.5 If a computer technician (or anyone working on information technology equipment) discovers any depiction of child pornography while installing, repairing, or otherwise servicing an item of electronic and information technology equipment, that worker must immediately report the discovery to their supervisor or the campus police. If reported to the supervisor, the supervisor must report it immediately to the campus police. Failure to do so is a business offence subject to fine of $1001.00

Acceptance of the Directive

By using the technology resources at the College of Lake County, it is assumed that the user agrees to abide by the policies that govern the use of the resources.

Enforcement

When an instance of unacceptable use is suspected, the college, with the approval of Vice President for Administrative Affairs, may investigate and take action to prevent their further occurrence. During an investigation, the college reserves the right to copy and examine any files or information resident on college systems allegedly related to improper use, including the contents of electronic mailboxes and voicemails. Investigations that discover improper use may cause the college's authorized investigators to:

- limit the access of those found using facilities or services improperly
- disclose information found during the investigation to other College authorities
- begin discipline actions as prescribed by college policies and procedures
- install automatic measures to limit improper use

Violations of these terms of technology use may result in revocation of technology privileges and/or in disciplinary action up to and including dismissal, as well as civil liability and/or criminal prosecution if user actions are also in violation of state and federal law. Unacceptable uses may also constitute a violation of the Electronic Communications Privacy Act of 1986, the Family Educational Rights and Privacy Act, defamation, copyright and/or trademark infringement laws and state or federal sexual harassment or discrimination laws.