Technology Use Policy

This AUP (Acceptable Use Policy) serves as notice to users, in compliance with Education Code Sections 48980 and 51871.5 that the Lassen County Office of Education's (LCOE) policies regarding information technology use, computer use, and access to the Internet and its communications systems for students, employees, and other authorized users. This policy will be reviewed and updated regularly to help ensure that LCOE adapts to changing technologies and circumstances.

ACCEPTABLE USE POLICY FOR DEVICE USE

In support of the Lassen County Office of Education's mission of supporting students for the future, LCOE provides computing, networking, and information resources to the campus community of students, faculty, and staff.

This AUP applies to the use of all LCOE computing and information technology resources of any kind. Additional computer and network use policies, terms, and conditions may be in place for specific electronic services offered by LCOE. The LCOE provides students, employees, and other authorized users with access to electronic resources.

Rights and Responsibilities

Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, the integrity of the systems, related physical resources, and observe all relevant laws, regulations, and contractual obligations.

It is the understanding that LCOE provides its employees with computers and network connectivity for the express purpose of fulfilling their professional and academic responsibilities. Any use of information technology resources deemed unacceptable is subject to disciplinary action.

Students and employees may have rights of access to information about themselves contained in electronic media, as specified in federal and state laws. Files may be subject to search under court order. In addition, system administrators may access user files, as required, to protect the integrity of information technology resources. For example, following organizational guidelines, system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, or that may have been corrupted or damaged.

Existing Legal Context

All Federal and State laws, as well as LCOE's rules, regulations, and policies apply. Applicable laws and regulations are not limited to those specific to information technology resources, but also include those that may apply generally to personal and professional conduct.

Misuse of computing, networking, or information resources may result in the restriction of privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable LCOE or school policies, procedures, or collective bargaining agreements.

Complaints alleging misuse of campus information technology resources will be directed to those responsible for taking appropriate disciplinary action. Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of the U.S. copyright law and is subject to civil damages and criminal penalties, including fines and imprisonment.

Examples of Misuse
Examples of misuse include, but are not limited to, the following activities:

- Using an information technology account that you are not authorized to use.
- Obtaining a password for an information technology account without the consent of the account owner.
- Using LCOE network to gain unauthorized access to any computer system(s) or to view files or information that you are not authorized to use.
- Removal, alternation, or destruction of sensitive or confidential information, including but not limited to personnel or student records.
- Knowingly performing an act that will interfere with the normal operation of information technology resources, including but not limited to devices, peripherals, or networks.
- Knowingly running or installing on any computer system or network or giving to another user; a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, malware, worms, or anything that might cause a denial or interruption of service.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws.
- Deliberately wasting information technology resources.
- Using electronic mail or other communications to harass others.
- Masking the identity of an account or machine.
- Posting materials to bulletin boards, social media sites, or to other information technology that violate existing laws or LCOE codes of conduct.
- Attempting to monitor or tamper with another user's electronic communications; reading, copying, changing, or deleting another user's files, or software without the explicit agreement of the owner.
- Use of information technology resources for commercial gain to the user or for purposes unrelated to the user's employment, education, or needs.
- Excessive personal use or personal use during work hours or instructional time, or personal use that interferes with the orderly conduct of LCOE in any way.

Activities will not be considered for misuse when authorized by appropriate LCOE officials, or their designees, for investigations, security, or performance testing.

ACCEPTABLE USE STANDARDS FOR INTERNET USAGE

The internet and communication systems may contain harmful matter as defined in section 313(a) of the Penal Code or may contain material considered by persons viewing it as harmful. Although LCOE exercises reasonable supervision over those who access the Internet and communication systems within our system, including exercising due diligence in educating students, employees, and other authorized users regarding acceptable and unacceptable practices on the Internet within our system, it is still possible that authorized users may intentionally or unintentionally access information which some may consider to be inappropriate or harmful.

Acceptable Use Policies
(A) The Lassen County Office of Education (LCOE) may terminate a user's account at any time without cause if these Acceptable Use Policies are violated, as deemed by LCOE or its designee.

(B) Use of the systems is a privilege, which may be terminated if the user abuses the system. Abuse would include but is not limited to: the placing of unlawful information on or through the system; the use or retrieval of information (messages, text, images, and programs) which is obscene, abusive, or otherwise objectionable;

redistribution or extension of Internet connectivity or systems beyond LCOE systems; and use of the system as a commercial operation or for personal gain.

(C) Users shall not transmit material that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment (cyber bullying), or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

Additionally, users are prohibited from engaging in cyberbullying. “Cyberbullying” means any severe or pervasive act or conduct inflicted by means of an electronic act, including, but not limited to: sexual harassment; hate violence; or harassment, threats, or intimidation directed toward one or more coworkers or students. Cyberbullying includes using another person’s electronic account for any of the purposes listed above.

An “electronic act” means the transmission of a communication, including, but not limited to, a message, text, sound, or image, or a post on a social networking website by means of an electronic device, including but not limited to, a telephone, wireless telephone, or other wireless communication device, computer, or pager.

(D) LCOE or designated staff will be the sole determiner of what constitutes use or retrieval of information (messages, text, images, programs), which is obscene, abusive, or otherwise objectionable.

(E) LCOE or designated staff reserves the right to access any material stored in its equipment on behalf of the user and reserves the right to remove any material which it considers obscene, abusive, or otherwise objectionable. There is no assumption of privacy.

(F) Users shall keep private their personal account access information (username and password), home addresses, phone numbers, Social Security numbers, and other individually identifiable information. They shall use the system only under their own user account and shall not assume a false or misleading identity or the identity of another user. Users shall lock or log out of LCOE technology equipment after each use to prevent unauthorized access to the account.

Users shall not use technological resources to post, publish, or transmit records, personally identifiable information (PII), or other confidential information related to students, employees, or privileged matters of LCOE to enable access by anyone not legally entitled or authorized by LCOE or designee to access it. PII includes, but is not limited to, information containing credit cards, driver license, bank account, and Social Security Numbers. The authorized transmission of such information shall be conducted using secure, encrypted means of transfer.

(G) Systems usage is guided by the generally accepted Internet practices called “netiquette,” a set of common-sense rules about using the Internet with respect for others.

(H) LCOE will certify each year that the requirements added by Children’s Internet Protection Act (CIPA) are being met. LCOE will educate staff, students, and guests about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms, and cyber bullying awareness reporting.

(I) LCOE will make reasonable efforts to maintain the integrity and effective operation of its systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communications, LCOE can assure neither the privacy of an individual user's use of the electronic resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored. In addition, California law provides that communications of LCOE personnel that are sent electronically may constitute

"correspondence" and, therefore, may be considered public records subject to public inspection under California's Public Records Act. There is no assumption of privacy when using any part of LCOE systems.

(J) The following items are indicative of and considered **Zero** tolerance violations:

1. Intentionally installing a malicious or viral file to infect the system.
2. Downloading or installing any unauthorized software to the computer or systems.
3. Altering or attempting to alter the computer's operating systems, software, or security systems.
4. Breaching or attempting to breach the system's security settings or devices.
5. Any act or attempted act that causes damage to the computer hardware/software and/or peripherals.
6. Any attempt to breach external sites or resources from LCOE systems without prior written approval from all entities involved.
7. Viewing or downloading inappropriate content from any source.
8. Any attempt made from a remote location to alter or disrupt LCOE's technology services.
9. Any attempt to threaten, harass, or bully another.
10. Sharing or distributing confidential or personal information, without prior written consent.

(K) Users shall not use non-LCOE issued external/internal drives or cloud storage systems to copy or transfer data. External drives include USB or Thunderbolt-connected flash drives, thumb drives, hard disk drives, cellular phones, tablets, and/or solid-state storage. The following Cloud Storage Providers are authorized for use with an LCOE user account: Microsoft Office 365, OneDrive, SharePoint (including all Office 365 services built on these platforms), Microsoft Azure Storage, and Google G-Suite for Education.

(L) All resources, applications, websites, social media, etc. need to be approved prior to use by LCOE Board, Superintendent, or their designee. Further, software that collects personal data must have a Data Privacy Agreement in place.

(M) LCOE may publish your (student/employee/other authorized user) name, pictures, video, or any other pertinent information for educational and promotional purposes on LCOE website, Facebook page, local newspaper, parent-teacher association, district/school newsletter, and similar parties. If you DO NOT wish for information, photographs, or videos to be released, please opt out in writing.

(N) This policy applies to all users using computers and/or equipment, or private home computers to access or utilize LCOE technology resources. The intent of LCOE is to use connections on the Internet only for reasons consistent with educational and business purposes. Anyone who uses the technology improperly may lose the privilege of using it, have a permanent record of such action, be disciplined, terminated, or expelled, and be financially liable. Using LCOE systems or software for any illegal use is prohibited. Any illegal use will be forwarded immediately to the authorities.

(O) Users shall not use technological resources to encourage the use of drugs, alcohol, or tobacco, to promote or participate in unethical practices such as cheating and plagiarism, or to conduct any activity prohibited by law, Board policy, or administrative regulation.

Users shall report alleged violations of the user obligations and responsibilities specified above, misuse of technological resources, and any security problems to LCOE or their designee.

A periodic review of storage resources including cloud storage will be performed by LCOE Information Technology Department as follows:

- LCOE may purge data or files deemed non-compliant with established regulations, policies, and/or guidelines, or those that pose a risk to LCOE
- Upon termination or permanent leave from LCOE, a user's individual data store will be transferred

to another use or deleted after 30 days

- Office 365 groups, SharePoint sites, and workgroup shares will be audited annually by LCOE, and any shared storage or groups that have not been accessed for more than a year will be archived or deleted

USE OF PERSONAL SOCIAL NETWORKING SITES – *FOR EMPLOYEES ONLY*

As an organization with a mission to support the education of young people and as a longtime leader in educational technology, LCOE's standards for appropriate online communication are necessarily high. One of the challenges of the digital age is that everything we write or post online leaves a long lasting and even permanent record that potentially can be seen by students, their families, and other members of LCOE's extended community. This is particularly true with social networking and media sites.

While the organization respects the right of employees to use social media and networking sites, as well as personal websites and blogs, it is important that employee's personal use of these sites does not damage LCOE's reputation, its employees, or its students or their families. Employees should exercise care in setting appropriate boundaries between their personal and public online behavior, understanding that what is private in the digital world often has the possibility of becoming public, even without their knowledge or consent. All online behavior should be consistent with the standards of professionalism expected of LCOE employees.

LCOE strongly encourages all employees to carefully review the privacy settings on any social media and networking sites they use (such as Facebook, Instagram, Twitter, LinkedIn, Reddit, etc.) and exercise care and good judgment when posting content and information on such sites. When using a social media site, an employee is encouraged to carefully consider the consequences if the employee includes current students, co-workers, or other work-related acquaintances as "friends," "followers," or any other similar terminology used by various sites. If an employee has a community that extends to persons who are parents or other members of LCOE's community, s/he must exercise good judgment and use professional, age-appropriate behavior regarding any content that I shared on the site. Additionally, employees should adhere to the following guidelines, which are consistent with LCOE's workplace standards on harassment, student relationships, conduct, professional communication, and confidentiality.

- An employee should not make statements that would violate any LCOE's policies, including its policies concerning discrimination or harassment;
- The employee must uphold LCOE's value of respect for the individual and avoid making defamatory statements about past or present employees or students, or their families;
- An employee may not disclose any confidential information of LCOE or any confidential information obtained during his/her employment about any individuals or organizations, including students and/or their families.

If LCOE believes that an employee's activity on social networking site, blog, or personal website may violate LCOE policies, LCOE may request that the employee cease such activity. Depending on the severity of the incident, the employee may be subject to disciplinary action.

GENERAL INFORMATION

Related policies are available online at www.lcoe.org website for clarification of policies and guidelines applying to the Lassen County Office of Education computing and communications resources, including this Acceptable Use Policy.

All users are referred to the following Board Policies and Administrative Regulations that also govern the use of technology and must be followed by all users of information technology:

Board Policy 4040 – Employee Use of Technology
Board Policy / Administrative Regulation 6163.4 – Student Use of Technology
Board Policy 5131 Conduct

CONSENT AND WAIVER

By signing the Consent and Waiver form, I agree to abide by the guidelines of LCOE Acceptable Use Policy and its rules and regulations. There is no assumption of privacy when using LCOE systems or services.

Further, I have been advised that LCOE does not have control of the information on the Internet. Other sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate, or potentially offensive. LCOE makes no warranties with respect to LCOE technology services and cannot assume any responsibilities.

The LCOE cannot be held liable for:

- The content of any information or advice received from a source outside LCOE or any costs or charges incurred as a result of seeing or accepting such advice;
- Any costs, liability, or damage caused by the way a user chooses to use his/her LCOE system;
- Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of LCOE.
- Use of LCOE systems must be consistent with LCOE's primary goals.
- Use of LCOE systems for illegal purposes of any kind.
- Use of LCOE systems to bully, distribute threatening, obscene, harassing materials.
- Use of LCOE systems to interfere with or disrupt network users, services, or equipment.
- Distribution of LCOE information and/or resources unless permission to do so has been granted by the owners or holders of rights to those resources.

As a public employee, the following are defined as a "gift of public funds" and are practices that are illegal:

- Use of LCOE telephones for personal long-distance and toll calls.
- Use of LCOE mail systems for personal use.
- Use or removal of LCOE equipment for personal use.
- Use of email, Internet, or computer network for personal use.
- Use or removal of LCOE supplies for personal use.
- Use of LCOE facilities for personal use.
- Use of LCOE systems for personal gain.

Print user's name | Date | User ID# (Office Use)

Signature of User | Date

Signature of Parent/Guardian | Date

Please sign and return this page.