

EMPLOYEE USE OF TECHNOLOGY**ACCEPTABLE USE POLICY – STAFF TECHNOLOGY**

This policy applies to the use of District-owned technology both inside and outside school premises. Within this policy, the "Acceptable Use Policy" ("AUP") refers to this document, and "technology" refers to, but is not limited to; laptops, desktop computers, Apple TVs, chrome books, iPads, copiers, two-way radios, telephones, mobile devices, projectors, printers, and peripherals including networks, internet, e-mail, voicemail, hand held pointing devices (mice), keyboards, printers, digital cameras, scanners, and video cameras. Staff members are expected to follow all of the policies outlined below when operating District-supplied technical resources.

This AUP was designed to establish clear and fair guidelines for the use of computer systems by the staff of Larkspur-Corte Madera School District (herein after: "LCMSD", or the "District"). Each staff member must abide by the guidelines set forth in this policy or forfeit their right to use this system. Violators of this policy may incur additional disciplinary action by the individual school, the District, and key violations will be reported to local, state, or federal authorities.

CONDITIONS OF USE

All District issued technology is District property and is provided to staff members for a period of time deemed appropriate by District Administration. As a condition of use, staff members must comply with and agree to all of the following:

1. Prior to being issued District technology, staff members will sign the attached acceptance form and agree to all outlined policies.
2. Staff members will use the computer systems only for work-related functions.

LCMSD has agreed to allow all staff the use of District-owned computer systems inside and outside each school in order to enhance, enrich, and facilitate teaching and administrative duties as well as school communications. The District's computer systems are to be used as a productivity tool for school-related business, curriculum enhancement, research, and communications only. Staff members shall exercise appropriate professional judgment and common sense when utilizing the District's computer systems, which includes the use of Chat, instant messaging software and Skype. The Superintendent or designee may decide that particular uses are or are not related to school employment or consistent with the objectives of the District.

Staff members are issued an electronic mail account upon hiring and are required to regularly read and respond to mail messages. This account is to be used for official school business only, including communications between teaching colleagues, parents, and administration. All communications sent or received regarding school related issues must be sent via a District-provided email account. Do not conduct business over personal email. Employee use of personal email accounts forfeits the right to privacy when used to conduct District business.

Use of the Internet and computer network access through LCMSD is a privilege, not a right. Violation of the AUP will result in the cancellation of privileges, discipline, up to and including termination, and/or possible legal action.

Each employee who is authorized to use district technology shall sign this Agreement, which indicates that the employee has read and understands this Agreement and Board Policy 4040 – Employee Use of Technology.

EMPLOYEE USE OF TECHNOLOGY

No frivolous use: All staff members connected to the network have a responsibility to conserve finite network bandwidth and storage capacity resources. As such, a staff member must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending unsolicited mass mailings or chain letters, spending excessive amounts of time on the Internet, using entertainment software such as games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic – anything that interferes with the performance of duties.

Blogging: Staff may be provided resources for publishing original content on the District's Intranet (internal) and the Web (public, external) servers. These resources may include tools and storage for publishing websites, blogs, wikis, or online course management systems (examples: Blackboard, Moodle, etc.). With the public potentially having access to content made available on our computer system, all staff members must engage in responsible use of these resources. These resources are provided with one single purpose: to promote communication as part of the learning process.

When utilizing Blogs, Discussion Boards, Wikis, Websites, and Online Course Management Systems:

1. Staff may not use obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening, or disrespectful language on websites, discussion boards, blogs, wikis or course management systems.
2. Staff may not knowingly or recklessly post false or defamatory information about a person or organization using the District's computer system including websites, discussion board, blogs, wikis, or course management systems.
3. Staff may not use the District's web servers to conduct business or engage in communications outside the realm of their assignment.

Student Data System Grade Book Access: Teachers are required to regularly upkeep student grades and report attendance using our electronic grading and attendance system.

Data Director: Data Director is a web-based data warehousing system that contains data from all Marin County databases all collected together in one place. For example, the Student Information System (SIS) and STAR assessment data are copied into Data Director. Teaching staff will be granted access to Data Director and will be required to fill out an additional Acceptable Use Policy before gaining access to this database.

Staff members shall NOT attempt to install software or hardware or change the system configuration including network settings without prior consultation with Tech Support.

LCMSD makes available a variety of software applications for staff use on its computer systems including browsers for interacting with websites and productivity software (word processing, spreadsheet, presentation, etc.) Only software that is purchased by LCMSD can be installed or used on District-owned computer systems. LCMSD makes no guarantee that any non-District-installed software will work now or in the future. If non-sanctioned software is detected on any District-owned computer it will be deleted during regular maintenance/troubleshooting and it will not be re-installed.

No external devices or malware: Staff members may not use external electronic devices that are not provided by the District (including laptop computers, phones, or other "Wi-Fi" devices) on the school network without approval from the Technology Department. Staff members are prohibited from installing, downloading, or distributing "malware," a class of software that includes viruses and Trojan

EMPLOYEE USE OF TECHNOLOGY

horses designed to interrupt or destroy services and data on the computer system.

Staff members are expected to protect school computer equipment from damage and theft. Staff members shall follow the following best practices:

1. Do not leave technology in an unlocked vehicle, even if the vehicle is in your driveway or garage. Never leave it in plain sight. If you must leave your laptop in a vehicle, leave it in a locked trunk. If you do not have a trunk, cover it and lock the doors.
2. Carry your laptop in a nondescript carrying case or bag when traveling.
3. Do not leave a meeting or conference room without your laptop. Take it with you.
4. Never check a laptop as luggage at the airport.
5. Lock the laptop in your office or classroom during off-hours or in a locked cabinet or desk when possible.
6. Regularly back up important data (such as grades, tests or exams) to your network folder or to a portable storage medium, such as CD-R or a flash-based memory stick (USB Thumb Drive). LCMSD Technology Department recommends staff back-up data on a weekly basis.
7. Do not place drinks or food in proximity to your computer.
8. Avoid extreme temperatures or sudden changes in temperature, which can damage a laptop.
9. When using a laptop, keep it on a flat, solid surface so that air can circulate through it. For example, using the laptop while it is directly on a bed can cause damage due to overheating.

Each staff member may be monetarily responsible for hardware damage to District property that occurs off school premises and/or software damage (including labor costs). Staff members will not be held responsible for computer problems resulting from regular school-related use; however, staff members will be held personally responsible for any problems caused by their negligence as deemed by the District's administration.

When using District technology or while connected to a District network, staff members shall not access, post, submit, or display inappropriate or illegal material.

Accessing, posting, submitting, or displaying the following material is strictly prohibited:

1. Inappropriate, threatening obscene, or sexually explicit content, including all forms of pornography.
2. Material that could be construed as harassment, intimidation, threatening, disruptive, defamatory, or discriminatory disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age disability, religion or political beliefs.
3. Material protected by trade secret or copyright law. Employees may not download, copy or make copyrighted material available to others for copying. Employees may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of LCMSD.
4. Any other material in violation of any United States or California state regulation.

Also, the following uses are strictly prohibited:

1. Unauthorized access to the files or equipment of others, accessing electronic resources by using another person's name or electronic identification, or sending anonymous electronic communications.
2. Unauthorized access to any data, documents, emails, or programs in the district's system.

EMPLOYEE USE OF TECHNOLOGY

3. Sharing confidential information or personally identifiable information with an open artificial intelligence system¹.
4. Use for commercial activities for personal profit or gain.
5. Use for product advertisement or political lobbying.
6. Subscribing to online fee-based services charged to the District without prior written approval.
7. Use of the system to engage in any activity deemed illegal by local, state, or federal statutes, including the selling or purchasing of illegal items or substances.

Staff members shall not compromise the computer system's security. Security on any computer system is a high priority, especially when the system involves many users. If you suspect a security problem on the network, you must notify the system administrator immediately.

1. Passwords are the property of the District. Passwords shall not be changed without prior authorization. If changed, the employee must immediately alert the District of the change and provide the new password. Passwords shall not be given to unauthorized staff members for any reason.
2. A staff member's account is only to be used by that individual. Attempts to log on to any device as a system administrator or other user will result in cancellation of user privileges. Any staff member that is identified as a security risk may have access privileges revoked.
3. Staff members may not reconfigure the security measures in place by the District to change access rights to computer files, or engage in activity that is considered "cracking", including: the use of proxy servers to bypass the Internet filter, changing the operating system permissions on files, attempting the use of "root kits" to gain administrative access to the computer system, or changing the access rights assigned to students by the network administrator(s).

Vandalism of any kind will not be tolerated. Vandalism in this AUP is defined as any malicious attempt to harm or destroy the data of another user, equipment, Internet, or networks that are connected to the Internet. This includes, but is not limited to, reading, deleting, copying, or modifying documents or files that belong to other employees without prior authorization on the computer system or the uploading or creation of computer viruses. Vandalism will result in cancellation of privileges.

DISCIPLINE

Any inappropriate use will result in the cancellation of privileges, discipline up to and including termination, and/or possible legal action. Based upon the acceptable use guidelines in this document, the system administrators will deem what is inappropriate use and their decision is final. The system administrators may close an account at any time. The administration of LCMSD may request the system administrator deny, revoke, or suspend specific user accounts.

INTELLECTUAL PROPERTY RIGHTS

Staff work performed within the scope of employment may entitle the District to intellectual property rights in the work. The District reserves the right to claim copyright to any such work as the employer.

NO EXPECTATION OF PRIVACY

Staff members are given computers and Internet access to assist them in the performance of their jobs. Staff members will have no expectation of privacy in anything they create, store, send, or receive using the District's computer system. Staff members expressly waive any right of privacy in anything they create, store, send, or receive using the District's computer system or Internet access. Staff members consent to allow the District:

¹ An "open artificial intelligence system" means a system with source code open to public viewing and editing.

EMPLOYEE USE OF TECHNOLOGY

1. Personnel access to and review of all materials created, stored, sent, or received by the staff member through any District network or Internet connection.
2. The right to monitor and log any and all aspects of its computer systems including, but not limited to, monitoring Internet sites visited by staff members, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by staff members including personal email. No inbound/outbound electronic communication is private and therefore will automatically be monitored for viruses, profanity, offensive language, racist and/or sexual comments, virus hoaxes, chain mail, and known spam mailers. LCMSD reserves the right to intercept, store, archive, delete, or view all emails for security/audit purposes and, where necessary, instigate appropriate proceedings against the parties involved. District personnel will report messages or material found relating to or in support of illegal or inappropriate activities to the proper authorities. Staff members will provide access to any computer system they have been assigned upon District's request.
3. All emails sent to LCMSD and its staff are subject to the California Public Records Act, as required by law, just as with all regular postal letters sent to the District or receipt of other documents. Emails sent to and from the Larkspur-Corte Madera's email system, shall be archived in accordance with the LCMSD's archival policy.

DISCLAIMER

The School Board is not responsible for any information that may be lost, damaged, or unavailable when using the computer system or for any information retrieved via the Internet. Furthermore, the School Board will not be responsible for any unauthorized charges or fees resulting from access to the computer system. Marin County Office of Education and the LCMSD accept no responsibility for any damage caused by receiving or sending emails from our email system. Marin County Office of Education scans all inbound emails, plus any attachments, for viruses but does NOT guarantee such messages to be virus-free. The onus is on the recipient to ensure they are indeed virus-free.

Exhibit adopted: February 2, 2005
Exhibit revised: October 28, 2015
Exhibit revised: December 18, 2024

LARKSPUR-CORTE MADERA SCHOOL DISTRICT
Larkspur, California

EMPLOYEE USE OF TECHNOLOGY

Acceptable Use Policy – Staff Technology - Acceptance Form

I have read and received a copy of the District’s Exhibit 4040 - Acceptable Use Policy – Staff Technology and understand my rights and obligations set forth within it. I understand that all computer systems the District has provided to me are the property of LCMSD. I will return the equipment to the District in the same condition in which it was provided to me.

I understand the use of the internet and all network accounts must be in support of education and research consistent with the educational objectives of LCMSD.

I understand that I may be personally responsible for damage to or loss of the assigned computer system. In case of my negligence that results in the damage or loss I will replace or pay the full cost of replacement of the damaged or lost equipment with equipment of equal value and functionality subject to the approval of the District.

I expressly waive any right of privacy in anything I create, store, send or receive using the District’s computer system or Internet access. I also understand that the technologists who operate LCMSD’s email system as well as our email provider (MCOE) have access to all mail, documents, and Internet access logs. I also understand that District personnel will report messages or material found relating to or in support of illegal or inappropriate activities to the proper authorities.

I understand that only software that is purchased by LCMSD can be installed or used on District-owned computers and if non-sanctioned software is detected on any District-owned computer it will be deleted during regular maintenance/troubleshooting and it will not be re-installed. I understand that I will not use a mobile device for District purposes while operating a motor vehicle unless the mobile device is hands-free approved. I certify that I have read, understand, and will abide by all terms outlined in this AUP. **I further understand that any violation of the regulations in the named policy may constitute revocation of these privileges, discipline up to and including termination, and/or possible legal action.**

Print Name: _____ Signature: _____ Date _____

Upon termination of employment or extended leave of absence, all technology belonging to the District must be returned in satisfactory condition to the District Technology Department.

Personal contact information:

Phone(s) _____ Email(s) _____

Date of hire: _____