

La Cañada Unified School District

Personnel Use of Technology Regulations (AR 4163.4)

Also known as the Staff Technology and Internet Use Policy

These regulations outline the acceptable use of computer, email and technology services at La Cañada Unified School District for district personnel. They have been put in place to protect both LCUSD and its employees. Inappropriate use of technology resources exposes LCUSD to risks including virus attacks, compromise of network systems and services, and legal issues. By using district provided computers and network services, employees agree to abide by these regulation. These regulations support and complement Board Policy 6163.4 Student Use of Technology, and Administrative Regulation 6163.4 Student Use of Technology and the Student Technology and Internet Use Agreement.

It is each district staff member's responsibility to:

- 1) Carefully read this document AR 4163.4 Personnel Use of Technology and BP/AR 6163.4 Student Use of Technology
- 2) Make sure students and parents/guardians have signed the Student Technology and Internet Use Agreement appropriate for their grade level before granting them access to district computers.
- 3) Take precautions to eliminate inappropriate access by closely supervising students' use of technology and ensuring that all users log in with their proper login names.
- 4) Direct questions to the district's director of technology if any part of the regulations or technology use agreements is unclear.

The district will make reasonable efforts to provide stable, reliable and functional network services through its technology department but cannot guarantee that such services will be fully operational 100% of the time due to limitations in resources and factors outside of its control. Effective network security is a team effort involving the participation and support of every LCUSD employee who deals with technology and/or information systems. It is the responsibility of every computer/network user to know these guidelines and to conduct activities accordingly. Failure to adhere to the rules and guidelines set forth in this document may result in the revocation of access to technology resources in the district as well as disciplinary measures.

1. The computers and the district network communication system (including the email system) are owned and operated by LCUSD and are maintained for the express purposes of teaching, information processing, and enhancing communication between district staff, parents, students, and community members, in the course of carrying out the district's educational mission.
2. District personnel may only access and use district network services from district provided computers and devices. In order to maintain the district's network security and to prevent the propagation of viruses and other malicious software, district employees are prohibited from plugging in any personal or non district owned and maintained computer or network equipment into the district's network. Employees seeking an exception to this rule must first obtain prior written approval from the district's director of technology, and there is no guarantee that such an exception will be granted.
3. District technology personnel are only authorized to service and maintain and support district owned computers. They are prohibited from servicing privately owned personal computer systems during the course of their work day due to liability and job responsibility reasons.
4. Users of the district's computer systems should be aware that the data they create or transmit on the district's systems including email, voice mail, and any computer files are not private and

remain the property of LCUSD. The district reserves the right to monitor all files and communications on district computers and network at any time without notice or consent.

5. The district's electronic , computer and internet systems and communications are intended to further its mission of educating students of the district. The district considers communication related to a staff member's professional duties as related also to the district's educational goals. However, the following email, internet (web browsing), and network communication activities are restricted or prohibited:
 - a) Intentionally accessing or transmitting harmful matter that is threatening, obscene, disruptive, or sexually explicit.
 - b) Sending large numbers of unsolicited email or network messages unrelated to the educational responsibilities of the sender, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
 - c) Transmitting harmful matter that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political belief via email or other network communication methods.
 - d) Soliciting of email for any other email address, other than that of the poster's account, with the intent to deceive, harass or to collect replies.
 - e) Creating or forwarding "chain letters", "public service announcements" or other "pyramid" schemes of any type. Typical messages might say "please forward this to everyone in your address book," or "send this to at least 10 people for good luck".
 - f) Mass emailing invitations, charity solicitations to district employees for personal or non-work related functions and events. (In the same way, district employees are not to use the printed district phone/address directory to send out mass mailings, invitations, and solicitations for non work related functions.)
 - g) The district permits limited personal email correspondence provided personal emails are brief and generated during off duty time. Personal emails must be simple, text-based, and not contain content that triggers or is likely to trigger a SPAM block.. Certain types of inbound personal correspondence are likely to generate email SPAM blocks and would require an excessive amount of time and effort for the technology department to process unblocking requests. Therefore, the technology department will not unblock and/or forward emails that are blocked and are related to the following personal uses: purchasing personal items or making travel arrangements unrelated to teaching using the district email account as the contact point, exchanging jokes, party invitations, and personal newsletters with friends via the district account, and receiving advertising or shopping update newsletters from retailers and internet based businesses. District employees are encouraged to use their personal email accounts at home to fulfill those functions and are asked to remove their name from any such distribution lists. All school related business related correspondence will continue to be unblocked upon request. By working together to minimize non-essential and non-professional email on the district's email system, more technology resources will be freed up to meet the ongoing technology needs of the district enabling timely, reliable, and responsive service.
 - h) Using the district's email, web, or network systems and resources for purposes related to financial, marketing, commercial or political activities.
 - i) Intentionally using the district's email and network systems to create, run, and/or send malicious software such as (but not limited to) viruses, spyware, keyloggers, or security circumventing programs.
 - j) Revealing one's own account password(s) to others or allowing use of one's account by others. This includes co-workers, teacher aides, parent volunteers, students, or family and other household members when work is being done at home. (Exceptions made for working with technology department staff to set up or troubleshoot a computer.)

- k) Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the distribution and/or installation of software products that are not appropriately licensed for use by LCUSD.
- l) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which LCUSD or the end user does not have an active license and beyond what is allowed under academic "Fair Use" guidelines.
- m) Effecting or enabling others to effect security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access.
- n) Conducting or promoting unethical practices or any activity prohibited by law, or district policy or regulation.

In the event there is a question or dispute about the meaning or scope of any of these rules or guidelines, final interpretation of these rules and guidelines will reside with the Assistant Superintendent for Facilities and Operations.

District Email Filtering policy

The district employs several email filtering and blocking programs in order to protect the district email system from email spam and virus attack. Any email containing an attachment with the following extensions will be *automatically blocked and deleted without warning or notice*: **.pif, .scr, .exe, .bat, .com, .cmd, and .cpl** since they are most often used by viruses. (this list may be changed without notice as needed to safeguard the district network. Staff may obtain the most current list from the district technology office.) Users who need to receive a file of one of those types will need first to notify techsupport@lcsd.net and then have the sender send that file and attachment to techsupport@lcsd.net with a request that the attached program be sent to the intended recipient in the subject line. (For example, SUBJECT: Please forward this attached program to Jane Doe, an employee at XYZ school. MESSAGE: The program is intended for use for the following purpose....) Tech support will evaluate the request to make sure it is appropriate for use on district equipment and is virus free. Once it passes inspection, the program will be placed in the user's file server folder and an email sent to the user indicating that the program has arrived and is ready for use.

In the event an email gets blocked by the GroupWise Anti Virus system (GWAVA), a notice will be sent to the user indicating that a message has been blocked by GWAVA. Reasons may be due to inappropriate ATTACHMENT – which indicates a virus was attached to the email, or SPAM – which indicates that the email is suspected of being a spam. Blocked email will only be retained by the system for 30 days, after which it will be automatically deleted. Some legitimate email may inadvertently get blocked by the filtering programs. Users may request (within 30 days) that legitimate email that was SPAM blocked be sent on through by **forwarding** the blocking notice to the district tech support staff at techsupport@lcsd.net. District tech support will make every effort to release the blocked email in a timely fashion but cannot guarantee an immediate turn around time due to work load and the number of requests. Blocked emails that are older than 30 days will not be recoverable since they will have been automatically purged from the system.

District Email Storage policy

Individual emails are limited to 2Mb in size including attachments, although exceptions may be granted for specific requests made to the system administrator. Each user will have up to 40Mb of space reserved for him/her on the email server to store current emails. In order to maintain an efficient email system and

to maximize limited technology resources, emails will be removed from the GroupWise server on a regular basis according to the following schedule:

Teachers:

- All emails received by a teacher (whether opened or not) will automatically be deleted from the Groupwise post office after they are 30 days old.
- Teachers who wish to keep an email beyond 30 days will have to manually move the email to their Groupwise archive before the email is purged. (This may be accomplished by right clicking on an email to be moved and selecting "Move to Archive")
- The archive location will be preset to the teacher's personal folder on the site's file server (a folder called Groupwise/Archive will be placed in each person's personal folder for this purpose). This removes archived email from the GroupWise post office so that Groupwise can run more efficiently while ensuring that a teacher's email archive is perpetually saved and available from his/her personal folder on the file server.
- Any email that has been moved to the GroupWise trash will be automatically purged from the Groupwise system after 14 days

Administrators and office staff:

- All emails will be automatically moved to the user's Groupwise archive in the user's personal folder (Groupwise/Archive) on the local file server after 90 days.
- Any email that has been moved to the Groupwise trash will be automatically purged from the Groupwise system after 14 days
- Administrators and office staff will be asked to manually clear their archives every summer of emails older than 365 days that are no longer of any use.

Confidentiality of Student Information

Students' rights to privacy are defined by the federal government in the Family Education Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA). It is the policy of this district never to include a photo of a student along with the student's name on any district sponsored website in order to protect the safety and privacy of the student. Furthermore, the district prohibits the publishing of any student work, student name, or photo of a student on a district or teacher webpage without express written permission from BOTH parent and student. Such permission must be received in writing and a copy of the permission sent to the district technology office for approval before any student work or photo of a student (without the students' names) is published on-line. A copy of a parental and student permission form may be obtained from the district technology office.

Ownership of teacher created materials placed on the District sponsored web site.

Teachers may develop extensive lesson plans or projects that they choose to make available on their district allotted teacher web page. For the purposes of copyright and material ownership, the district recognizes that any such material developed independently by the teacher may belong to the teacher and that the teacher may exercise ownership right and publication rights to that material in the future. However, if the material is subject to ownership or copyright, the author grants the district a nonexclusive license granting full use of such materials at no cost in perpetuity, in exchange for the district hosting the materials on its website. In other words, by placing content on a district sponsored web space, a teacher is granting a license to the district to use any and all of that content for the district's educational purposes at no cost either now or in the future. The district may not sell such work, and the teacher is free to submit that work for commercial publication in the future with the provision that the district may continue to use that work indefinitely at no cost.

Superintendent's Approval: _____ Date: _____

La Cañada Unified School District
Personnel Use of Technology Regulations (AR 4163.4)
Also known as the Staff Technology and Internet Use Policy

I HAVE READ AND UNDERSTAND THE LCUSD PERSONNEL USE OF TECHNOLOGY REGULATIONS (AR 4163.4). I SHALL ABIDE BY THEM AND UNDERSTAND THAT ANY VIOLATION IS UNETHICAL AND MAY EVEN CONSTITUTE A CRIMINAL OFFENSE. SHOULD I COMMIT ANY VIOLATION, MY ACCESS PRIVILEGES SHALL BE REVOKED AND DISCIPLINARY ACTION AND/OR APPROPRIATE LEGAL ACTION SHALL BE TAKEN.

Signature _____

Date _____

Print Name _____

School _____