

ACCEPTABLE USE OF TECHNOLOGY

The Los Angeles County Superintendent recognizes and supports advances in technology. While these technologies provide a valuable resource to the Office, it is important that the Office's use of technology be appropriate for Office purposes. Inappropriate use of Office technology may result in loss of employee productivity, service, compromised security, lost data, and other negative consequences.

Definitions

“Authorized Possessor of an Office-owned portable device” means the possessor of Office-owned portable devices (including but not limited to tablets, laptops, cellular phones, and flash drives) who the Office has authorized to possess those devices. Office-owned portable devices may be given to staff members to carry out the Office’s mission. Upon receipt of an Office-owned portable device, the staff member is the authorized possessor as defined by the California Electronic Communications Privacy Act (also known as CalECPA or SB 178). Staff members understand and acknowledge that the Office may, at any time, without cause, confiscate and/or electronically access any Office-owned portable device and search the electronic information stored therein. Upon such confiscation or electronic access, the staff member is no longer the authorized possessor of the Office-owned portable device.

“Office computing devices” include computers, mobile devices, tablets, and any other Office-owned equipment that stores, generates, or transmits information in an electronic form.

“Office network communication systems” include but are not limited to, the Office email system, phone system (including voicemail), the Office’s on-line collaboration and file storage services, cloud network and cloud systems, and the computer network including internet access through the network.

“Office technology” includes Office computing devices and Office network communication systems. Office technology, including the data and products of its use, is the property of the Office.

“Users of Office technology” include each and every employee, student, parent, volunteer, contractor, or other individual who has been authorized to possess or use Office technology.

Specific Consent

Use of Office technology by each and every employee, student, volunteer, contractor, or other individual shall constitute that person's acknowledgment of and agreement to abide by this policy. Users of Office technology grant specific consent, as defined by CalECPA, to the Office to review and monitor electronic communication information and electronic device

ACCEPTABLE USE OF TECHNOLOGY (continued)

information created, stored, or transmitted on the Office's computing devices and network communication systems. Users of Office technology should be aware that any data they create, store, or transmit on the Office's network communication systems are not private and remain the property of the Office. The Office reserves the right to monitor all files, programs, applications, internet traffic, and communications that reside on Office computing devices, servers, and cloud systems or travel over its network communication systems at any time without additional notice or consent.

Office technology is the property of the Office. Use of Office technology is a privilege and also a requirement, not a right. Users of Office technology shall not have an expectation of privacy in their use of Office technology. The Office reserves the right to monitor use of Office technology to ensure public resources are appropriately used for Office-related business and to ensure that the Office's policies and regulations regarding harassment and nondiscrimination as well as other applicable policies and regulations, are being followed. Any use of Office technology for personal use must be minimal and not interfere with Office business or job duties.

Users of Office technology shall not engage in prohibited uses, as defined in the regulation to this policy. Any violations of this policy or regulation shall result in consequences up to and including disciplinary, civil, and/or criminal action.

Office supervisors are required to consistently and uniformly enforce the Acceptable Use of Technology policy, regulation, and agreement, as well as procedures provided by the Department of Technology Services.

The Superintendent, or designee shall establish an Acceptable Use of Technology Agreement that outlines the obligations and responsibilities of users of Office technology. Upon employment, and whenever significant changes are made to the Office's Acceptable Use of Technology Agreement, employees shall be required to acknowledge in writing or via electronic signature that they have read and agreed to the Acceptable Use of Technology Agreement.

Employees are expected to review, understand, and abide by the Acceptable Use of Technology policy, regulation, agreement, and any accompanying procedures provided by the Department of Technology Services. These documents are legally binding on employees, whether or not they have signed the Acceptable Use of Technology Agreement. Any employee who violates any provision of the Acceptable Use of Technology policy, regulation, agreement, or procedures shall be considered as having acted in an individual capacity and outside the scope of employment, and, as such, may be subject to disciplinary action, up to including termination or criminal prosecution by government authorities.

ACCEPTABLE USE OF TECHNOLOGY (continued)

Employees are required to use office accounts when conducting agency business and not personal accounts. Staff provided stipends to use their personal phone/device must still use office accounts when conducting business on their personal phone/device. Such staff should also recognize that the Public Records Act applies to agency communications regardless of whether the device used is an agency device or a personal device. In addition, text messages are not archived by the office, however, staff may be asked to search for and provide text messages on their devices and sign a sworn statement to that effect, as part of a Public Records Act Request.

(cf. 6163.4 - Student Use of Technology)
(cf. 1114- LACOE Approved Social Media)

*Legal Reference:***EDUCATION CODE**

52295.10-52295.55 *Implementation of Enhancing Education Through Technology grant program*

GOVERNMENT CODE

3543.1 *Rights of employee organizations*

PENAL CODE

502 *Computer crimes, remedies*

632 *Eavesdropping on or recording confidential communications*

VEHICLE CODE

23123 *Wireless telephones in vehicles*

23123.5 *Mobile communication devices; text messaging while driving*

23125 *Wireless telephones in school buses*

UNITED STATES CODE, TITLE 20

6751-6777 *Enhancing Education Through Technology Act, Title II, Part D, especially:*

6777 *Internet safety*

UNITED STATES CODE, TITLE 47

254 *Universal service discounts (E-rate)*

CODE OF FEDERAL REGULATIONS, TITLE 47

54.520 *Internet safety policy and technology protection measures, E-rate discounts*

*Management Resources:***WEB SITES**

CSBA: <http://www.csba.org>

American Library Association: <http://www.ala.org>

California Department of Education: <http://www.cde.ca.gov>

Federal Communications Commission: <http://www.fcc.gov>

U.S. Department of Education: <http://www.ed.gov>

ACCEPTABLE USE OF TECHNOLOGY

Committees shall be established to review and approve procedures and standards for acceptable use, security, and operation of Office technology.

- A. Users of Office technology grant specific consent, as defined by CalECPA, to the Office to review and monitor electronic communication information and electronic device information created, stored, or transmitted on the Office's computing devices and network communication systems. The Office reserves the right to monitor the use of Office technology and all files, programs, applications, internet traffic, and communications that reside on Office computing devices, servers, and cloud systems or travel over its network at any time without additional notice or consent to ensure that:
 - 1. Public resources are appropriately used for Office-related business;
 - 2. Applicable Office policies and regulations including those regarding harassment and nondiscrimination are followed;
 - 3. Any personal use of Office technology does not interfere with Office business or job duties and is minimal in terms of use and cost.
 - 4. Any use complies with federal and state law.

- B. The Office may require new registration, account information or password changes from any person to continue services, either on a regular basis or without notice. Passwords are to be kept confidential at all times and not be given out to anyone, including the Technology Services Helpdesk, colleagues, students, supervisors or administrators.
 - 1. Users shall not leave their workstation unattended while they are logged on without locking it.
 - 2. Users shall use the password feature of their screen saver.
 - 3. Users shall not allow anyone to log into an account using their logon credentials. If a person does not have the proper capabilities to do a task, he/she should contact Technology Services so appropriate capabilities (such as delegate access) can be provided.

- C. The Office reserves the right to periodically purge electronic mail messages stored on the Office server.

ACCEPTABLE USE OF TECHNOLOGY (continued)

- D. Users of Office technology shall not have an expectation of privacy in any matter created, received, stored in or sent from Office technology, including password-protected matter, all of which may be public records.
- E. A parental approval form is required for each student allowed access to Office technology, specific computers or the Internet. Parents and students shall be provided with LACOE Board policy 6162.4 and 6162.7 describing how students will be expected to use the equipment and what will constitute unacceptable behavior.
- F. Electronic mail use must be in accordance with guidelines established by the Communications Division. Electronic mail messages for broadcast to all employees must be approved by the Division Director or a designee prior to being sent to the electronic mail account designated for this purpose.
- G. Employees will report all incidents of unacceptable use immediately without inquiry to their supervisor who will report it to the appropriate division for handling. All incidents of viruses, malicious software or security failures shall be reported immediately to the Help Desk and any other relevant LACOE division.
- H. Office-owned portable devices may be issued to staff members to carry out the Office's educational mission. If provided, the employee must use the Office-owned portable device when conducting Office business and may not use his or her personal device for that purpose. If the employee uses a personal phone for which a stipend is received, the employee agrees that any work related material belongs to LACOE. Further, the Office reserves the right to remove Office-related content from any personal device electronically or manually. The authorized possessor of Office-owned portable devices are personally expected to:
 - 1. Keep the device free from illegal content or material inappropriate for the school setting; and
 - 2. Ensure that Office-owned portable devices are not used by family members or friends for personal use.
- I. Users of Office technology should not use personal accounts for conducting agency business and electronic communication, nor to load applications, programs, and other resources onto Office computing devices unless authorized by Technology Services. In all cases users must exercise prudent judgment to ensure that only approved and properly licensed applications, programs, and other resources appropriate for the school setting are loaded onto Office computing devices. Users of Office technology should not expect personal applications, files, and accounts (including but not limited to personal email accounts or social media accounts) residing on Office computing devices or the Office's network communication systems to remain private. The Office reserves the right to inspect, delete, and report any applications, programs, files,

ACCEPTABLE USE OF TECHNOLOGY (continued)

or other information that find their way onto Office devices or Office network communication systems.

- J. Employees are required to use office accounts when conducting agency business and not personal accounts. Staff provided stipends to use their personal phone/device must still use office accounts when conducting business on their personal phone/device. Such staff should also recognize that the Public Records Act applies to agency communications regardless of whether the device used is an agency device or a personal device. In addition, text messages are not archived by the office, however, staff may be asked to search for and provide text messages on their devices and sign a sworn statement to that effect, as part of a Public Records Act Request.
- K. Prohibited uses of Office technology include the following:
1. Using LACOE technology for commercial advertising, gain, or fraud
 2. Using LACOE technology for unauthorized personal or non-profit purposes
 3. Political activities
 4. Religious activities
 5. Intentionally disabling or bypassing security systems or procedures
 6. Unauthorized use of another's passwords or computer to access files, resources, or systems or unauthorized use of an account belonging to another user
 7. Unauthorized access to protected systems containing student, personnel, financial or other data
 8. Using Office technology to access, obtain or distribute confidential, personal or private information without authorization or unauthorized possession of any data that might be considered a violation of these rules in paper, magnetic, or other form
 9. Using Office computers to copy software or using software in violation of copyright or license agreements
 10. Copying Office software, files or documents for personal use or downloading or installing personal or unauthorized software on Office computers
 11. Unauthorized use or possession of services, real property, or intellectual property

ACCEPTABLE USE OF TECHNOLOGY (continued)

12. Sending, creating, intentionally receiving or storing any material in violation of any United States or California law or LACOE policy. Such material includes, but is not limited to
 - a. Copyrighted, trademarked or patented material
 - b. Threatening, racist or discriminatory, sexist, or obscene material. "Obscene material" is defined as (a) the subject as a whole appeals to the prurient interest (shameful or morbid interest in nudity, sex, or excretion) of the average person, using contemporary community standards; (b) the works depicts or describes in a patently offensive way sexual conduct proscribed by the state statute, and (c) the work as a whole lacks serious literary, artistic, political, or scientific value
 - c. Material protected by privilege, trade secret, privacy or confidentiality laws
 13. Forging documents or electronic mail messages or using Office technology to create, send or receive messages using someone else's user name or address or portraying someone else as the originator of the message or document without authorization
 14. Sending or forwarding chain letters, is defined as correspondence directing the recipient to send out multiple copies
 15. Using LACOE technology to either create a computer virus or other malicious software or to knowingly initiate a computer virus or other malicious software on the network or other LACOE technology
 16. Using the network or electronic mail in a manner inconsistent with other Office policies, regulations or procedures
 17. Intentionally disrupting network traffic or degrading or disrupting equipment and system performance. Users shall not plug in any unauthorized equipment on the network (wireless access points, etc.) unless approved and authorized by Technology Services.
- K. Consequences for violations of the policy or regulation, include the following:
1. Suspension or revocation of access to Office technology
 2. Suspension or revocation of network privileges, including electronic mail
 3. Disciplinary action, up to and including termination

ACCEPTABLE USE OF TECHNOLOGY (continued)

4. Civil or criminal action against the offender, where appropriate

Warranties of Security or Services

LACOE makes no warranties of any kind, whether expressed or implied for Office Technologies, including network services, LACOE will not be responsible for any damages or losses suffered while using LACOE technologies. These damages include loss as a result of delays, non-or misdeliveries, or service interruptions caused by the system, errors, or omission.

Use of any information obtained via the network is at the individual's own risk. LACOE specifically disclaims responsibility for the accuracy of information obtained through its network services.

Users may encounter material on the Internet that is controversial and which user, parents, teachers, or administrators may consider inappropriate or offensive. It is the user's responsibility not to initiate access to such material. Any efforts by LACOE to restrict access to Internet material shall not be deemed to impose any duty on LACOE to regulate access to material on the Internet.

The Los Angeles County Office of Education makes no warranties with respect to network services, particularly the Internet, and specifically assumes no responsibilities for:

- A. The content of any advice or information received by a user from a source outside the county of any costs or charges incurred as a result of seeking or accepting such advice.
- B. Any costs, liabilities, or damages caused by the way the user chooses to use network access.
- C. Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of LACOE.
- D. While LACOE supports the privacy of electronic mail, users must assume that this cannot be guaranteed.

Electronic Mail

Electronic mail is a valuable tool at LACOE that improves communication of many types of information.

- A. All electronic mail messages, like all paper documents, are the property of the County Office, and are subject to Office policy, procedures, and control.

ACCEPTABLE USE OF TECHNOLOGY (continued)

- B. Electronic mail is for official Office use only- not personal use. Electronic mail is not a confidential forum for communications. The contents of messages may be monitored, and all users should be aware that every message can be stored, forwarded, and printed. As such, electronic mail messages become public documents available to the general public and subject to discovery in any legal proceedings.
- C. The major purpose of electronic mail is informal communications; e.g., calendaring meetings, notes, reminders, phone messages, simple questions, or other similar purposes.
- D. Electronic mail messages should not contain profanity, racial, or sexual slurs, or other unprofessional language.
- E. Employees are responsible for keeping access to their electronic mail account secure and may be held accountable for any messages sent using their electronic mail account. Each user is expected to change their password of first use and every 90 calendar days thereafter and keep it secure. Continued use of a generic password, leaving a password where it can be found, giving the password to anyone or leaving a computer unattended with electronic mail open can result in someone else sending messages in the owner's name. Automatic logging on to electronic mail without password entry for each use should not be used.
- F. LACOE will comply with all state and federal laws as well as LACOE policies and regulations governing retention of email, including email which may be classified as business records, employee records, public records or student records.

Broadcast to All Electronic Mail Users

- A. Prior to sending any message to all electronic mail users, the message must be reviewed by the appropriate Cabinet member as to its appropriateness. The initials of the approving shall appear at the end of the announcement to show it has been approved.
- B. Electronic mail should not be used for mass circulation announcements, minutes, event publicity and other similar purposes to all LACOE staff on the system, without prior approval by the appropriate Cabinet member. This includes sales, fund-raisers, or the birth or death announcements of non-employees and relatives of employees, unless approved in advance by the division head or Assistant Superintendent.
- C. Inter-group announcements, such as birth, death, or marriage notices, are to be used only within an individual division with prior approval of the division head. With the approval of the division head, they may be sent to other division heads who will determine the distribution within their divisions.

ACCEPTABLE USE OF TECHNOLOGY (continued)

- D. A specific address has been established for broadcast electronic mail. Approved messages are sent to this address. Network staff will broadcast only approved messages.

Personnel

SE 4040(a)

ACCEPTABLE USE OF TECHNOLOGY AGREEMENT

Receipt of Selected Superintendent Policies and Regulations

I have received a copy of Superintendent Policy 4040 and the associated regulations.

I understand that I am expected to comply with and abide by them. I am aware that a complete copy of all policies and regulations is available online and/or through my supervisor. I will review them.

The following statements are provided in accordance with Superintendent Policy 4040:

Employees are required to use office accounts when conducting agency business and not personal accounts. Staff provided stipends to use their personal phone/device must still use office accounts when conducting business on their personal phone/device. Such staff should also recognize that the Public Records Act applies to agency communications regardless of whether the device used is an agency device or a personal device. In addition, text messages are not archived by the office, however, staff may be asked to search for and provide text messages on their devices and sign a sworn statement to that effect, as part of a Public Records Act Request.

I understand that as a user of Office technology I grant specific consent, as defined by CalECPA, to the Office to review and monitor electronic communication information and electronic device information created, stored, or transmitted on the Office's computing devices and network communication systems. The Office reserves the right to monitor the use of Office technology and all files, programs, applications, internet traffic, and communications that reside on Office computing devices, servers, and cloud systems or travel over its network at any time without additional notice or consent to ensure that:

1. Public resources are appropriately used for Office-related business;
2. Applicable Office policies and regulations including those regarding harassment and nondiscrimination are followed;
3. Any personal use of Office technology does not interfere with Office business or job duties and is minimal in terms of use and cost;
4. Staff is in compliance with federal and state law.

I recognize that the Office will periodically access my Office-owned cellular telephone, computer (laptop and/or desktop), and/or other office computing, cloud systems/servers and communication devices to perform the following functions:

1. Repair or maintenance of the device

ACCEPTABLE USE OF TECHNOLOGY AGREEMENT (continued)

2. Upgrade of the device
3. Retrieve information in response to the Public Records Act
4. Retrieve records in compliance with the Pupil Record Act, Education Code section 49062, et seq., FERPA, and AB 1584
5. Fulfill the Office's statutory duties and Board Policies to maintain public records
6. Conduct administrative searches of the device if appropriately authorized.
7. Monitor employee compliance with state and federal law and Office policy

I further understand that Office-owned portable devices may be given to staff members to carry out the Office's educational mission. The employee must use the Office-owned portable device to conduct Office business and may not use his or her personal device for that purpose. If the employee uses a personal phone for which a stipend is received, the employee agrees that any work related material belongs to LACOE. Further, the Office reserves the right to remove Office-related content from any personal device or associated cloud service, electronically or manually. The authorized possessor of Office-owned portable devices shall:

1. Keep the device free from illegal content or material inappropriate for the school setting; and
2. Ensure that Office-owned portable devices are not used by family members or friends for personal use.

Users of Office technology should not use personal accounts to load applications, programs, and other resources onto Office computing devices unless authorized by Technology Services. In all cases users must exercise prudent judgment to ensure that only authorized and appropriately licensed applications, programs, and other resources appropriate for the school setting are loaded onto Office computing devices. Users of Office technology should not expect personal applications, files, and accounts (including but not limited to personal email accounts or social media accounts) residing on Office computing devices or the Office's network communication systems to remain private. The Office reserves the right to inspect, delete, and report any applications, programs, files, or other information that find their way onto Office devices or Office network communication systems.

I understand that it is my responsibility to:

1. Report lost or stolen devices, including devices that contain private Office information, to the Division of Technology Services within 24 hours of discovery of the loss

ACCEPTABLE USE OF TECHNOLOGY AGREEMENT (continued)

2. Report faulty or malicious abnormalities that occur on Office technology to the Division of Technology Services
3. Protect my user identification, password, information, and system from unauthorized use
4. Respect the intellectual property rights of authors, contributors, and publishers in all media
5. Adhere to the terms of software licenses and other contracts. Persons loading software on any Office-owned device must adhere to all licensing requirements for the software. Except where allowed by the licenses, copying software licensed for Office use for personal use is a violation of the Acceptable Use of Technology policy and regulation. Only authorized staff should load software onto office-owned devices.
6. Adhere to all other applicable Office policies and/or collective bargaining agreements
7. To use Office technology in a manner that complies with State and Federal law

I understand that the following are prohibited uses of Office technology:

1. Using Office technology for commercial advertising, gain, fraud
2. Political and/or religious activities
3. Intentionally disabling or bypassing security systems or procedures
4. Unauthorized use of another's passwords or computer to access files, resources, or systems, or unauthorized use of an account belonging to another user
5. Unauthorized access to protected systems containing student, personnel, financial, or other data
6. Using Office technology to access, obtain, or distribute confidential, personal, or private information without authorization; or unauthorized possession of any data that might be considered a violation of these rules in paper, magnetic, or other form
7. Using Office technology to copy software, or using software in violation of copyright or license agreements
8. Copying Office software, files, or documents for personal use, or downloading or installing personal or unauthorized software on Office devices
9. Unauthorized use or possession of services, real property, or intellectual property

ACCEPTABLE USE OF TECHNOLOGY AGREEMENT (continued)

10. Sending, creating, intentionally receiving, or storing any material in violation of any United States or California Law or Office policy. Such material includes, but is not limited to:
 - a. Copyrighted, trademarked, or patented material
 - b. Threatening, racist or discriminatory, sexist, or obscene material. “Obscene material” is defined as (a) the subject as a whole appeals to the prurient interest (shameful or morbid interest in nudity, sex, or excretion) of the average person, using contemporary community standards; (b) the works depict or describe in a patently offensive way sexual conduct proscribed by the state statute; and (c) the work as a whole lacks serious literary, artistic, political, or scientific value
 - c. Materials protected by privilege, trade secret, privacy, or confidentiality laws
11. Forging documents or electronic mail messages or using Office technology to create, send, or receive messages using someone else’s user name or address, or portraying someone else as the originator of the message or document without authorization
12. Sending or forwarding chain letters, defined as correspondence directing the recipient to send out multiple copies
13. Using Office technology to either create a computer virus or other malicious software, or to knowingly initiate a computer virus or other malicious software on the network or other Office technology
14. Using the network or electronic mail in a manner inconsistent with other Office policies, regulations, or procedures
15. Intentionally disrupting network traffic, or degrading or disrupting equipment and system performance.
16. Plugging in any unauthorized equipment in Office devices or on the Office network (wireless access points, etc.) unless approved and authorized by Technology Services.

I understand that the consequences for violation of the Acceptable Use of Technology policy or regulation include the following:

1. Suspension or revocation of access to Office technology
2. Suspension or revocation of network privileges, including electronic mail
3. Disciplinary action, up to and including dismissal
4. Civil or criminal action against the offender where appropriate

ACCEPTABLE USE OF TECHNOLOGY AGREEMENT (continued)

I understand that I shall have no expectation of privacy when using Office computing equipment or technological resources, including but not limited to Office provided email, file storage systems, and other communication and collaborative services.

I understand that any Office or school records maintained on any of my personal devices, or messages sent or received on a personal device that is being used to conduct Office business may be subject to disclosure pursuant to subpoena or other lawful request.

I also understand that in order to comply with state and federal student privacy laws, I will not allow people who are not Office employees (such as parents, volunteers, or students) to use or access my Office issued computing device since confidential or protected student information or sensitive Office email communications may be stored or accessed from there.

Receipt of Selected Superintendent Policies and Regulations

I have received a copy of Superintendent Policy 4040, the associated regulation, and this Acceptable Use of Technology Agreement.

I have read and understand these documents. I agree to comply with and abide by them.

Division

Print Name

Signature

Date