SAN DIEGO COUNTY OFFICE OF EDUCATION		**ADMINISTRATIVE REGULATION NO. 3600**
CLASSIFICATION:	**Business and Noninstructional Operations**	**ADOPTED: 9/09/97**
		REVISED: 10/13/21
SUBJECT:	**Use of Technological Resources**	**PAGE: 1 of 8**

The county superintendent of schools encourages employees' use of technological resources in the performance of their work assignments. This administrative regulation presents the obligations and responsibilities of employees and other authorized adults in the use of San Diego County Office of Education (SDCOE) technological resources. This regulation implements the Internet safety requirements of the Children's Internet Protection Act (CIPA) to safeguard minors and ensure eligibility for Universal Service (E-rate) discounts on Internet access, telecommunications services, and other eligible products and services.

The county superintendent of schools assigns responsibility for the secure, reliable, and efficient operation of SDCOE technological resources to the assistant superintendent, Integrated Technology Services. As necessary, he/she shall establish, implement, and disseminate to employees and other authorized users written operating procedures consistent with the requirements of this administrative regulation.

For purposes of this regulation, "technological resources" refers to all equipment; software; electronic networks, both wired and wireless; electronic communications; websites and content; cloud services; and licenses that are owned, leased, or operated by SDCOE. Exhibit 1 presents definitions of SDCOE technological resources.

"Users" means employees or other authorized users of SDCOE technological resources. Authorized users may include temporary employees or other individuals who are granted access to specified technological resources in accordance with requirements and procedures established and administered by the assistant superintendent, Integrated Technology Services.

Employees and other authorized users of SDCOE technological resources (users) are responsible for their proper use at all times. Users are expected to use technological resources to more effectively perform the duties and responsibilities of the operations and programs of SDCOE.

Users should be aware that computer files, Internet use, and communications over electronic networks, including e-mail, chat, text messages, social media, and voice mail, are not private. The county superintendent of schools or his/her designee may access and/or monitor use of SDCOE technological resources at any time without advance

notice or consent. Information maintained on SDCOE technological resources, including archived e-mail and files deleted from a user's account, is the exclusive property of SDCOE and may be accessed by the county superintendent of schools or designee, or required to be disclosed under the California Public Records Act or by court order.

In compliance with Federal Communications Commission rules for CIPA, the assistant superintendent, Integrated Technology Services, or designee, shall ensure that Internet access of all SDCOE computers is regulated by a technology protection measure (Internet filter) and that the operation of such measure is maintained. The technology protection measure shall continuously filter and block access to visual depictions that are obscene, child pornography, or harmful to minors. The assistant superintendent, Integrated Technology Services, or designee may disable the technology protection measure during use of a computer by an adult to enable access for bona fide research or other lawful purpose.

No employee or other authorized user may permit minors to use computers with Internet access where the technology protection measure is not enabled. Use of SDCOE technological resources by minors is governed by Administrative Regulation 6163, Student Use of Technology.

Acceptable Use Agreement

This administrative regulation constitutes the *SDCOE Acceptable Use Agreement*. Before being granted access to SDCOE technological resources, and on an annual basis thereafter, employees and other authorized users shall be required to read and sign the *SDCOE Acceptable Use Agreement*. The Executive Director, Human Resources, or designee shall be responsible for ensuring compliance with this requirement.

Users are required to maintain the highest standards of professional and ethical conduct and to comply with the *SDCOE Acceptable Use Agreement*, applicable laws, County Board of Education policies, SDCOE administrative regulations, and Integrated Technology Services operating procedures when using technological resources. If an employee is uncertain about whether a particular activity constitutes proper use, he/she

should refer to Administrative Regulation 4020, Code of Ethics, or other relevant Board policy or administrative regulation, or consult with his/her supervisor for guidance.

The county superintendent of schools or designee shall provide employees opportunities for professional development in the appropriate use of SDCOE technological resources.

User Obligations and Responsibilities

Employees and other authorized users shall use the technological resources of SDCOE, as defined in Exhibit 1 of this administrative regulation, in accordance with the obligations and responsibilities specified below.

1. 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 SDCOE technology equipment after each use to prevent unauthorized access to the account.

2. 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 SDCOE to enable access by anyone not legally entitled or authorized by the county superintendent of schools or designee to access it. PII includes, but is not limited to, information containing, credit card, driver license, bank account, and Social Security Numbers. The authorized transmission of such information shall be conducted using secure, encrypted means of transfer.

3. Users shall not use technological resources for commercial or other for-profit activities, for political or religious purposes, for unauthorized solicitations, to encourage the use of drugs, alcohol, or tobacco, to promote unethical practices, or to conduct any activity prohibited by law, SDCOE Board policy, or administrative regulation. Use of technological resources to send chain letters or unsolicited bulk email, known as spam, is prohibited.

4. Users shall not access, download, post, publish, transmit, or display in electronic form harmful or inappropriate material that is threatening, obscene, disruptive, sexually explicit, or child pornography, or that could be construed as harassment or disparagement of any member of a group protected by state or federal law.

5. Users are prohibited from using technological resources to engage in harassment, intimidation, or threats of any kind to students, staff, administrators, or any other individuals.

   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.

6. Users shall not use technological resources to download, store, post, transmit, or publish copyrighted material, including multimedia and software, except as permitted by copyright law or with appropriate permission or license.

7. Unless authorized to do so by the county superintendent of schools or designee, users shall not knowingly access and without permission read, delete, copy, or modify other users’ electronic mail messages or files; interfere with other users’ ability to send or receive electronic mail messages; or forge or fraudulently use other users’ electronic mail account or files.

8. Unless authorized to do so by the county superintendent of schools or designee, users shall not forward their SDCOE domain email messages to a non-SDCOE email account, including but not limited to Yahoo, Gmail, AOL or any other domain.

9. If an employee uses a personally owned device to access district technology or conduct district business, he/she shall abide by all applicable laws, County Board of Education policies, SDCOE administrative regulations, and the *Acceptable Use Agreement*. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

10. If an employee chooses to voluntarily use a personally owned device to access SDCOE applications that are protected by Multi-Factor Authentication (MFA), they must first install the SDCOE-approved MFA application on their personally owned device for authentication. Employees who opt-in to use their personally owned device(s) understand that the use of their personally owned device to conduct official SDCOE business is for personal convenience and is not required by SDCOE.

11. Users shall not use SDCOE technological resources to commit acts of vandalism.

    "Vandalism" includes, but is not limited to, hacking, intentionally uploading, downloading, transferring, or creating computer viruses and/or any malicious or unauthorized use of SDCOE technological resources. Also included are any actions that attempt to harm or destroy equipment or materials or manipulate the data, in any form, of any other user. Public offenses related to computer crime are further defined in Penal Code section 502.

12. Users shall not purposefully disable or circumvent any technology protection measure installed on SDCOE technological resources.

13. Users shall not participate in social networking websites unless, for purposes consistent with their work assignments, they are authorized to do so by their division assistant superintendent. Creation of SDCOE program, department, or division social media accounts requires approval by the Communications department. Participation in social networking websites must be in strict compliance with the *SDCOE Acceptable Use Agreement*. Access to social

networking websites must be approved by the assistant superintendent, Integrated Technology Services.

14. To protect the security and reliability of the SDCOE wireless network, users are prohibited from installing any wireless network in facilities owned or operated by SDCOE. Any exceptions must be approved in advance by the assistant superintendent, Integrated Technology Services.

15. Users shall not use non-SDCOE issued external drives 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.

16. Users shall not use any cloud storage system that is not explicitly authorized by the assistant superintendent, Integrated Technology Services, or his/her designee. The following Cloud Storage Providers are authorized for use with an sdcoe.net 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.

17. Users shall not transfer files containing personal information (data) between an SDCOE-owned device and non-SDCOE-owned device or cloud storage account that is not sanctioned by SDCOE for any reason.

Users shall report alleged violations of the user obligations and responsibilities specified above, misuse of technological resources, and any security problems to the assistant superintendent, Integrated Technology Services, or designee.

User privileges may be terminated, denied, suspended, or revoked at any time and/or the user may be subject to disciplinary and/or legal action in the event of violation of any conditions of the *SDCOE Acceptable Use Agreement*, applicable law, Board policy, administrative regulation, or Integrated Technology Services operating procedures.

The assistant superintendent, Integrated Technology Services, or his/her designee may implement controls to enforce and/or audit the use terms defined in this regulation.

A periodic review of storage resources including cloud storage will be performed by the Integrated Technology Services (ITS) department as follows:

- ITS may purge data or files deemed non-compliant with established regulations, policies, and/or guidelines, or those that pose a risk to SDCOE
- Upon termination or permanent leave from SDCOE, 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 ITS, and any shared storage or groups that have not been accessed for more than a year will be archived or deleted

Annual Review

The assistant superintendent, Integrated Technology Services, or designee, shall annually review and update this administrative regulation and relevant procedures for the use of SDCOE technological resources to adapt to changing technologies and circumstances.

Compliance with CCPA

Notwithstanding any other federal, state, or local law, SDCOE and any of its third-party vendors involved in receiving, processing, or storing student information shall comply with all applicable requirements of the California Consumer Protection Act (CCPA). For purposes of the CCPA and this administrative regulation, "personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonable be linked, directly or indirectly, with a person or household. A more comprehensive definition of what personal information is and includes can be found in *Exhibit 1 – Definition of Terms*.

Board Policy: 2303, 3560, 3600, 4004, 4019, 4022

Administrative Regulation: 2300, 3513.2, 3560, 4019, 4020, 4021, 4030, 6163

Derivation: Adopted 9/9/97, Public Hearing 2/4/03, Amended 2/4/03, Technical Revision 10/20/03, Amended 11/6/09, 4/5/13, 8/12/20, 10/13/21.

Legal Reference:

Education Code
200 et seq., 260, 32261, 48900 et seq., 48980, 51006 - 51007, 51870 - 51874
Government Code
6250 - 6270.7, 11135
Penal Code
311, 313, 422.55 - 422.6, 502, 632, 653.2
United States Code, Title 15
Children's Online Privacy Protection Act (COPPA), sections 6501 - 6502
United States Code, Title 17
101 - 122
United States Code, Title 18
2256
United States Code, Title 20
6751 - 6777
United States Code, Title 47
254(h), 254(l)
Children's Internet Protection Act (CIPA), section 1721 et seq.
Protecting Children in the 21st Century Act, section 215
Code of Federal Regulations, Title 34
100.3
Code of Federal Regulations, Title 47
54.500 - 54.520
FCC 01-120 Report and Order, Adopted March 30, 2001
11-125 FCC Report and Order, Adopted August 10, 2011
Public Law 107-110
No Child Left Behind Act of 2001, sections 2401- 2441
Public Law 110-385
Broadband Data Services Improvement Act, sections 211, 215

Management Resources:

California Department of Education: *Federal Telecommunications Discounts for Schools and Libraries* - www.cde.ca.gov/ls/et/ft/eratemain.asp
Federal Communications Commission: www.fcc.gov
USAC Schools and Libraries Division (SLD): www.sl.universalservice.org/
San Diego County Office of Education Integrated Technology Services Operating Procedures: teams.sdcoe.net/infosecurity.asp

DEFINITIONS OF TERMS

For the purposes of Administrative Regulation 3600, Use of Technological Resources, technological resources of the San Diego County Office of Education (SDCOE) refers to equipment, software, electronic networks, websites and content, and licenses that are owned, leased, or operated by SDCOE including, but not limited to the following:

1. Equipment: All desktop, laptop, tablet, and portable computers; telephones and cellular phones; personal digital assistants (PDAs), and peripheral devices, including printers, scanners, and external or removable storage devices.

2. Software: Operating systems; off-the-shelf applications; operating system and browser extensions; and the CD-ROMs, DVDs, and electronic downloads containing applications and installers.

3. Software as a Service (SaaS): Application software that is Internet-based and is not installed on local workstations, such as Google G-Suite for Education and Microsoft Office 365.

4. Electronic Networks: Equipment, cabling, software, and data circuitry that provide wired and wireless connections among SDCOE facilities, commercial Internet access (including services granted by the K-12 High Speed Network), and interconnection of SDCOE servers and workstations.

5. Electronic Communications: Any transfer of signals, writings, images, sounds, data, or intellectual property that is created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or more electronic communications systems utilized via an SDCOE electronic network. Examples include, but are not limited to, e-mail, electronic messaging, “tweets” (Twitter), streaming media, chat messages, instant messages, and web site content.

6. Websites and content: All websites hosted on equipment owned or leased by SDCOE and all websites bearing the San Diego County Board of Education copyright, including the underlying text, pictures, data, and presentation of information that comprises static and dynamic web page content.

7. Licenses: All documentation, activation keys and codes, and rights to use and/or redistribute that are purchased by or granted to SDCOE for the purpose of using copyrighted software.

8. Multi-Factor Authentication (MFA): A security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. MFA combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods.

9. Personally Owned Device: A piece of electronic equipment that can connect to the internet and is not owned by SDCOE. Such devices may include, but are not limited to laptops, desktops, tablets, smartphones, and/or other computing devices.

10. Personal Information includes, but is not limited to the following:

    (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

    (B) Any categories of personal information described in subdivision (e) of Section 1798.80 of the California Consumer Privacy Act of 2018.

    (C) Characteristics of protected classifications under California or federal law.

    (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

    (E) Biometric information.

    (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

    (G) Geolocation data.

    (H) Audio, electronic, visual, thermal, olfactory, or similar information.

    (I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Personal Information does not include publicly available information, or information that is lawfully made available from federal, state, or local government records.

ACCEPTABLE USE QUICK REFERENCE GUIDE:

1. Only San Diego County Office of Education (SDCOE) related data and files can be stored on our infrastructure. SDCOE assumes no responsibility for the loss, protection, or restoration of personal data.

2. Employees are strongly urged to store all date, information, or files that are created or managed as part of their work function in OneDrive or SharePoint shares. These platforms support version control and can synchronize date between your device and the cloud.

3. Your department may have additional requirements on how the data is managed, such as file naming conventions, structure of folders, version retention, etc.

4. Unless you have been directed by your manager or there is a specific business need to store sensitive information, no such data relating to you or someone else can be stored, transmitted, or used on SDCOE resources. Sensitive information is that which contains, credit card, driver license, bank account, or Social Security Numbers, or other personal identifiable information.

5. Materials that are subject to a copyright where SDCOE or user does not have a license for such materials should not be stored on SDCOE resources.

6. Periodically, and at the discretion of each department's business procedures, all employees should review and audit data accessible in their individual data store, departmental, and workgroup shares, and delete any files that are no longer needed in accordance with AR 3560, Records Retention and Disposition. Data storage is a finite resource that needs to be managed proactively and has detrimental impact to the infrastructure if it goes unchecked.

7. Files and folders should be named appropriately and uniquely for ease of management and discovery should a restoration of data be required.

8. Data backups of individual data stores, departmental, and workgroup shares on non-cloud systems are performed on a daily basis. Data can be restored as far back as 30 days from the time they were deleted or modified.

9. When using Cloud storage for collaboration with others, either from within SDCOE or elsewhere, only grant access to files or folders that are required for the collaboration to take place. Access to data should be given on a strictly need to know basis.