AR 4040 Personnel

Employee Use Of Technology

Stanislaus County Office of Education Technology Services:
User Obligations and Responsibilities

Employees are authorized to use SCOE equipment to access the Internet, e-mail or online services in accordance with County Office policy and the user obligations and responsibilities specified below. Use of County Office technology is a privilege granted to employees and students; it is not a right. These guidelines and provisions are subordinate to local, state and federal statutes.

1. The employee in whose name a network account is issued is responsible for its proper use at all times. Employees shall keep account information, home addresses, telephone numbers and any sensitive information private. Employees shall use the system only under their own network account userid.
2. Employees shall use the system responsibly, for lawful and work-related purposes.
   a. Employees shall not leave their workstation without locking it.
   b. The County Office is not responsible for financial obligations arising through the unauthorized use of County Office technology resources including, but not limited to, the purchase of products or services or the use of personal devices while on County Office property. Employees will be financially liable for any damage or network disruption resulting from negligence or misuse. Personally owned devices that connect to the County Office network and technology resources are subject to the stipulations in this policy.

   (cf. 6162.7 - Use of Technology in Instruction)

3. Employees shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability or religion.
   a. Employees County Office educators will select and preview materials and websites used for instructional purposes. However, they cannot be expected to preview all sites that students may encounter while performing online research.
   b. To the extent possible, the County Office will block access to unmonitored social media and inappropriate or offensive websites. Due to the open design of the Internet and networked computer systems, users are warned that they may occasionally receive content that may be offensive to them. Users should report all such occurrences to the Technology Services Department.
4. The County Office may monitors all usage of technology to protect technology resources for safety purposes and for cybersecurity purposes.
   a. Designated County Office staff have the authority to conduct a reasonable investigation into alleged misconduct, including an Internet search of public content, which includes social media sites, as defined by California Education Code section 49073.6, for evidence of such misconduct. The purpose of such an investigation would be to protect the safety of County Office students.

5. Employees supervising students are responsible to supervise, educate and monitor student usage of the Internet and network use to protect students from harmful matter or unlawful activities.

6. Employees shall not disclose confidential student information through use of technology resources in a manner which violates either the California pupil privacy laws (Education Code 49060) or the Federal Education Rights Privacy Act (FERPA) (20 USC 1232g).

   (cf. 4030 - Nondiscrimination in Employment)

   (cf. 4031 - Complaints Concerning Discrimination in Employment)
   (cf. 4119.11/4219.11/4319.11 – Sexual Harassment)

7. Employees shall not use the system to promote unethical practices or any activity prohibited by law, County Office policy or administrative regulations.
   a. The County Office technology resources shall not be used by employees for political lobbying activities as defined under Education Code section 7054 nor for commercial purposes. County Office acquisition policies will be followed for purchase of goods or services through technology resources.
   b. Employee account privileges may be modified, disabled or terminated at any time without prior notice.
   c. Employee access to technology resources will be disabled after separation from employment.

8. Copyrighted material shall not be placed on the system without the author's permission. Employees may download copyrighted material only in accordance with applicable copyright laws.
   (cf. 6162.6 - Use of Copyrighted Materials)

9. Employees shall not intentionally upload or download unauthorized software, shareware and freeware nor create or spread computer viruses or other malware. Employees shall not maliciously attempt to harm, disrupt, degrade or destroy County Office network, equipment, materials or websites or the data of any other user, including so-called "hacking," Examples including, but not limited to: packet sniffers, password cracking programs, or port scanners.
   a. Intentionally disrupting network traffic or degrading or disrupting equipment and system performance shall not be permitted. Employees shall limit activities, such as streaming media that uses excessive network resources and bandwidth that could disrupt network services to other employees and students.
   b. Employees shall not tamper with computers, devices, networks, printers or other County Office equipment.
   c. Employees shall not take equipment (hardware or software) home without prior written permission of the County Superintendent or designee.
   d. Employees shall not connect any unauthorized equipment or devices to the network unless approved and authorized by Technology Services.
   e. County Office provides ample file and data storage for employees. All work-related confidential records and files shall be stored on County Office network.
   f. Employees shall not use third party nor cloud services unless provided by the County Office.
   g. Employees shall not use unencrypted portable storage devices such as flash drives or external hard drives.
   h. Employees shall not subscribe or use fee-based online services without prior written approval of the County Office Superintendent or designee.

10. Employees shall not read other user's electronic mail or files. They shall not attempt to interfere with other users' ability to send or receive electronic mail, nor shall they attempt to read, delete, copy, modify or forge other users' mail. Employees must not share their access or use other users' accounts, passwords, login procedures, personal identification numbers (PINS), security tokens, or similar information.

11. Employees shall not log in as another user or attempt to circumvent security procedures of the County Office network.
    a. If an employee does not have the proper capabilities or authorization from their immediate supervisor to do a task, the user should contact immediate supervisor and Technology Services to request appropriate access.

12. Employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the County Office or using County Office equipment or resources without permission of the Stanislaus County Superintendent of Schools or designee. (Examples of sites include, and is not limited to: YouTube, Google sites, Facebook, Twitter, Blog sites, etc.) Approved sites shall be subject to rules and guidelines established for County Office online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of many of these sites, any such site shall include a disclaimer that the County Office is not responsible for the content of the messages. The County Office retains the right to delete material on any such online communications. A web resource which the public might reasonably assume is a County Office resource should be identified as such and have County Office approval. Employees who develop or maintain web resources not hosted by the County Office should make it clear that it is not an official County Office site.

13. Employees shall use the County Office approved resources only to communicate with students, parents and other entities. Employees may not use personal technology tools and resources, accounts or other personal resources for communication and interaction with students, parents and the community. If personal tools and resources are used for work-related purposes, those communications and interactions may be discoverable under state or federal public records laws.

14. Employees may not represent the County Office nor post comments to the internet representing the view of the County Office without permission from the County Superintendent or designee.
    (cf. 1113 - District and School Web Sites)

15. Users shall report any security problem or misuse of the County Office services to the County Superintendent or designee. Employees shall report any system weakness which may result in unintentional disclosure of information or security threats to Technology Services.

16. Employees may not make unauthorized copies of copyrighted or County Office owned software or resources.

17. Employees who take County Office owned devices or other resources offsite shall take reasonable precautions to ensure the safety, security and confidentiality of sensitive data. Employees shall employ security procedures recommended by Technology Services. This may include the use of a Virtual Private Network (VPN), passwords, encryption or other current best practices. Any loss of County Office owned devices or other resources shall be reported immediately to immediate supervisors and to Technology Services. Employees shall not store sensitive data on unencrypted usb drives and storage devices, or personal cloud services.

18. Minimal personal use of internet access is allowed at SCOE within the following parameters:
    a. This access is restricted to County Office approved users only and shall not include family members or others not affiliated with the County Office.
    b. Use shall not interfere with the normal performance of an employee's work duties. Such use may occur during non-duty times and shall not occur during work hours.
    c. Such use shall not result in direct costs to SCOE, cause legal action against, or be detrimental to the County Office. Minimal use shall not degrade or materially affect the operation of County Office network resources.

19. Any questions or issues regarding the Employee Acceptable Use Policy and procedures should be directed to the Division Director of Human Resources. Violation of any conditions of use described herein may be cause for disciplinary action or termination of employment. When and where applicable, law enforcement agencies may be involved.

20. Email is provided to County Office employees and is a valuable tool in improving communications. It is to be used for work-related purposes. Messages become public documents available under the public records laws and subject to inspection under the California Public Records Act.
    a. Mailbox space should be kept to a minimum. Unneeded messages should be deleted.

Employees are expected to follow SCOE's Social Media Protocol (Exhibit B 4040)

(c.f. 6163.4 – Student Use of Technology)

21. Employees shall not register students for websites and applications that collect student data for marketing or advertising purposes.

22. Employees shall not register students for websites or applications that collect personally identifiable information including, but not limited to: first and last name, home or physical address, online contact information, username, telephone number, photo, video, or audio file containing the child's image, voice or geolocation.

Legal References:

EDUCATION CODE

48980 Required notification at beginning of term

51006 Computer education and resources

51007 Programs to strengthen technological skills

51870-51874 Education technology

51870.5 Student Internet access

52270-52272 Education technology and professional development grants

60044 Prohibited instructional materials

PENAL CODE

313 Harmful matter

502 Computer crimes, remedies

632 Eavesdropping on or recording confidential communications 653.2 Electronic communication devices, threats to safety

GOVERNMENT CODE

3543.1 Rights of employee organizations

LABOR CODE

2870 Rights to an invention

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 15, 6501-6506 Children's Online Privacy Protection Act Title 20

Title 20, 6777 Internet Safety (Children's Internet Protection Act, CIPA)

CODE OF FEDERAL REGULATIONS

Title 16, 312.1-312.12 Children's Online Privacy Protection Act

Title 47, 54.520 Internet safety policy and technology protection measures, E-rate

Management Resources:

CSBA PUBLICATIONS Cyberbullying: Policy Considerations for Boards, Policy Brief, July 2007

WEB SITES

CSBA: http://www.csba.org

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

California Coalition for Children's Internet Safety: http://www.cybersafety.ca.gov California Department of Education: http://www.cde.ca.gov

Center for Safe and Responsible Internet Use: http://csriu.org

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

Federal Trade Commission, Children's Online Privacy Protection: http://www.ftc.gov/privacyinitiatives/childrens.html

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

Web Wise Kids: http://www.webwisekids.org

Common Sense Media: http://www.commonsensemedia.org

Regulation STANISLAUS COUNTY OFFICE OF EDUCATION

approved: February 4, 2003 Modesto, California

revised: August 23, 2011

revised: March 7, 2018