Employee Use of District Technology

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

District technology includes, but is not limited, to the district's Internet/Intranet/Extranet-related systems, email system, phone system including voice mail, video conferencing, computers, the computer network including Internet access through the network, storage media, and office equipment. Use of district 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 regulation. District technology, including the data and products of its use, is the property of the district.

1. The District reserves the right to monitor the use of district technology without notice and consent to ensure that:

a. Public resources are appropriately used for district-related business;

b. Applicable district policies and regulations, including those regarding harassment and nondiscrimination, are followed;

c. Any personal use of district technology does not interfere with district business or job duties and is minimal in terms of use and cost.

2. The district may require new registration, account information or password changes from any person to continue services, either on a regular basis or without notice. Passwords should not be given to any individual except authorized district personnel and supervisors. Passwords should not be stored in easily accessible areas, i.e., under keyboards, on monitors, or in desk drawers. Users shall not login others using their personal user ID or password credentials.

3. The district reserves the right to periodically purge electronic mail messages stored on the district server.

4. Users of district technology shall not have an expectation of privacy in any matter created, received, stored in, or sent from district technology, including password-protected matter, all of which may be public records.

5. 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 Board Policy 238 describing how students will be expected to use the equipment and what will constitute unacceptable behavior.

6. Electronic mail use must be in accordance with guidelines established by the District. Electronic mail messages for broadcast to all employees must be approved by a district administrator or a designee prior to being sent to the electronic mail account designated for this purpose. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

7. Employees will report all incidents of unacceptable use immediately without inquiry to their supervisor who will report it to the Assistant Superintendent of Human Resources and Instruction or Assistant Superintendent, Business Services, for handling. All incidents of viruses, malicious software or security failures shall be reported immediately to the IT Help Desk and the Assistant Superintendent, Business Services.

8. All the rules of conduct described in the school's campus code and district's policies and regulations apply on the Internet and other on-line services. The user in whose name an on-line services account is issued is responsible for its proper use at all times. Users shall keep personal account numbers, home addresses, and telephone numbers private. They shall use the system only under their own account.

9. Unauthorized staff, volunteers, parents, family members, or significant others may not configure, diagnose, or repair any district equipment. Only district approved personnel shall be authorized to perform this work.

10. Security systems that are not approved by the District are strictly prohibited; i.e., CMOS passwords, unapproved wireless access points, or third party security applications. If such systems are discovered, the equipment shall be erased and configured to district standards.

11. Prohibited uses of district technology include the following:

a. Using district technology for commercial advertising, gain, or fraud;

b. Using district technology for unauthorized personal or non-profit purposes;

c. Political activities;

d. Religious activities;

e. Intentionally disabling or bypassing security systems or procedures;

f. Unauthorized use of another's passwords or computer to access files, resources or systems, or unauthorized use of an account belonging to another user;

g. Unauthorized access to protected systems containing student, personnel, financial, or other data;

h. Using district 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, magnet, or other form;

i. Using district computers to copy software or using software in violation of copyright or license agreements;

j. Copying district software, files or documents for personal use or downloading or installing personal software on district computers for non-district purposes;

k. Unauthorized use or possession of services, real property, or intellectual property;

l. Sending, creating, intentionally receiving or storing any material in violation of any United States or California laws or district policy. Such material includes, but is not limited to:

(1) Copyrighted, trademarked, or patented material;

(2) Inaccurate, disruptive, 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 work 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;

(3) Any material that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs;

(4) Material protected by privilege, trade secret, privacy, or confidentiality laws.

m. Forging documents or electronic mail messages or using District technology to create, send, or receive message using someone else's user name or address or portraying someone else as the originator of the message or document without authorization;

n. Sending or forwarding chain letters which is defined as correspondence directing the recipient to send out multiple copies;

o. Using district 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 district technology, or any other processes that would damage computers, computer systems or computer networks;

p. Using the network or electronic mail in a manner inconsistent with other district policies, regulations, or procedures;

q. Intentionally disrupting network traffic or degrading or disrupting equipment and system performance;

r. Accessing or exploring on-line locations, chat rooms such as "myspace", yahoo chat, etc., materials or on-line games that do not support the curriculum and/or appropriate for school-related work;

s. Vandalizing and/or tampering with equipment, programs, files, system performance, or other components of the network, including copying, distributing, or modifying copyrighted software;

t. Causing congestion on any technological system or interfering with the work of others, e.g., engaging in chain letters, unapproved chat rooms or in peer-to-peer networking applications such as Napster, Gnutella, etc., broadcasting messages to lists or individuals, modifying or deleting files;

u. Attempting to infiltrate or "hack" into any technological system, or interfering with another person's ability to use that system, including password sniffing, using a keylogger, and/or port scanning;

v. Using unauthorized fee-based services on the internet or via the phone system for dial-up connections;

w. Intentionally wasting finite resources, e.g., on-line games, instant messaging;

x. Coaching, helping, observing, or joining any unauthorized activity on any technological system;

y. Posting anonymous messages, unapproved web pages, or unlawful or libelous information on the system;

z. Granting remote or local control of a networked system to a third party.

12. Technology equipment (hardware or software) may not be taken, or copies to be taken, home or off-site without written permission signed by a district administrator.

13. The district may provide the staff with a district-issued cell phone for employment-related purposes, including emergency situations, and for personal use. Employee telephone expenses that result from use which is not related to district business, is personal in nature, and is not otherwise deemed as emergency or essential by the employee's supervisor, shall be subject to reimbursement from the employee to the district within 60 days of use. As an alternative, the employee may pay the district a flat rate monthly fee of $15.00 as reimbursement for personal use of a district-issued cell phone. Monthly reimbursement shall be provided via payroll deduction (Form 4045-1).

14. Personal or non-district purchased hardware and software will not be allowed to connect or integrate into the district network unless stipulated by another board regulation.

15. Donated hardware and software must meet minimum standards and licensing requirements from the district IT department and must have board approval.

16. Consequences for violations of the policy or regulation include the following:

a. Suspension or revocation of access to district technology;

b. Suspension or revocation of network privileges, including electronic mail;

c. Disciplinary action, up to and including termination;

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

Regulation COMPTON UNIFIED SCHOOL DISTRICT

approved: November 24, 2015 Compton, California