Pueblo City Schools (District 60)

Policy and Procedures

File: GBEE
Author: Geri Patrone
Date: 6/14/2012
Section: G
Category: B
Sub-Category: EE
Title: Staff Use of Technology and Internet and Electronic Communications

This policy was EHD and recoded 12/99
This policy was retitled on 6/14/2012

Staff Use of Technology and Internet and Electronic Communications

Introduction
Pueblo School District No. 60 (hereafter referred to as "the District") provides staff (including District employees, consultants, contract employees and volunteers working at the District) and guests access to the network, servers, computers, other devices, software, services, communication systems and connections to the Internet that it owns, leases or contracts for use (hereafter referred to as "District Technology") to the extent needed to support its educational mission.

While using technology on or near school property, in school vehicles and at school-sponsored activities, as well as using District Technology resources from off-site locations, each staff member and guest is expected to act in an appropriate manner consistent with school, District, and legal guidelines. District staff working with students is also expected to remind students about their responsibilities and to reinforce and exemplify these expectations when using technology.

Blocking or filtering obscene, pornographic and harmful information
Access to the Internet enables access and use of extensive online material. Some of this material may contain items that are illegal, defamatory, inaccurate, profane, sexually oriented, or offensive to some people. The District does not condone or permit access to inappropriate material and uses content filtering technology to protect, to the extent reasonably possible, against Internet access by both adults and minors to visual depictions that are obscene, pornography or harmful to minors. District staff and guests should be aware that content filtering tools are not completely fail-safe and while at school, students using District Technology or accessing the Internet through the District's network should be supervised as closely as possible. Staff and guests who encounter inappropriate or offensive material while using the Internet or electronic communications must make this content no longer visible and immediately notify their supervisor and contact the Technology Service Desk to report the issue.

No expectation of privacy
Computers, servers, network and other devices that are District-owned or used for District operations are intended to be used only for educational purposes. The District reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of District computers and computer systems, including all Internet and electronic communications and materials, and information transmitted or received. District staff may review files and communications to maintain system integrity and ensure that staff and guests are using District Technology responsibly.

Electronic communications sent and received by District staff and guests using District Technology may be considered a public record subject to public disclosure or inspection under the Colorado Open Records Act. All such electronic communications shall be monitored to ensure that public electronic communication records are retained, archived and destroyed in accordance with applicable law. Staff and guests shall have no expectation of privacy when using District Technology, the Internet or electronic communications, and should not expect that files stored on, or sent via, the District's or its vendors' servers and networks will be private. All material and information accessed and received through the District's computers and systems shall remain the property of the District.

Acceptable and unacceptable uses of technology

Staff and guests shall use District Technology in a responsible, efficient, ethical and legal manner. Because technology and ways of using technology are constantly evolving, every unacceptable use of technology at the District cannot be specifically described in policy. Examples of unacceptable uses include, but are not limited to, those listed immediately below and in subsequent sections of this document.

Staff and guests shall not use District or Personal Technology to:

- harass, threaten, demean, bully or promote violence or hatred against another person or group of persons, or to promote or advocate the destruction of property,
- transmit or post false or defamatory information about a person or organization,
- violate the privacy of others by taking or transmitting unauthorized photographs or videos,
- disclose, use or disseminate personal information regarding minors without authorization from the appropriate administrator,
- transmit or post information that, if acted upon, could cause damage or disrupt the educational programs or operations of the District,
- disrupt school operations and activities (including obtrusive ringing or buzzing of devices during instructional time or other school-sponsored activities),
- commit plagiarism, represent the work of others as one's own or someone else's, use copyrighted ©, registered ® and/or trademarked ™ materials without attribution, or assist others to do any of the preceding,
- access fee services without specific authorization from the appropriate administrator,
- use District Technology for purposes not related to district education objectives, including financial gain, advertising, entertainment, commercial transactions or political purposes,
- transmit or post criminal speech or speech in the course of committing a crime, including threats to individuals or groups, instructions on breaking into computer systems or networks, child pornography, drug dealing, purchase of alcohol, gang activities, etc.,
- illegally transmit or store copyrighted material and material protected by trade secret, or
- perform any activity that violates District Board of Education policy, a school rule, or a local, state or federal law.

Staff shall not allow others to have unsupervised access to their District-issued laptops or Internet-ready devices.

Staff and guests wanting to use Personal Technology at the district shall not

- connect or attempt to connect Personal Technology to the District network for purposes other than to store or retrieve education-related data or make appropriate use of District Technology resources,
- connect or attempt to connect Personal Technology to the District network other than through the wireless network provided for guests and for employees' and students' use of Personal Technology,
- connect or attempt to connect peripherals not owned by the District to a District device without prior approval by Technology Services and the staff member's administrator, with
- the administrator being responsible for any resulting damage to District Technology and providing for any subsequent support using school or department resources.

Security

The security of District Technology and data is vital to the District. Staff who suspects a security problem must immediately notify their supervisor and the Technology Service Desk. Staff and guests must not demonstrate or discuss such problems with anyone other than their supervisor and Technology Services staff engaged in addressing the matter.

Staff and guests are expected to take measures to protect District Technology, access and data by

- safeguarding technology devices and equipment in their possession and in their work area from unauthorized access and theft,
- logging off or locking active sessions when leaving the immediate vicinity of a computer,
- providing the minimum level of network access to sensitive or confidential data to the smallest number of people needed to meet District needs on a timely basis, and
- limiting and monitoring access to stored data that is sensitive or confidential, whether it is printed, saved on an external device or recorded on digital media.

Staff and guests shall not

- attempt to discover or use another person's password or any other identifier,
- reveal or offer to reveal their personally-assigned access credentials to another person,
- impersonate another user or conceal their identity on District Technology,
- use override credentials to enable a student to bypass internet filtering,
- attempt to gain unauthorized access to any District Technology or other system, or
- attempt to read, alter, delete or copy data, files or electronic communications of another user, except for staff directed to do so by the appropriate administrator.

Any user identified as a security risk, or as having a history as such with other computer systems, may have their access to the Internet and District Technology restricted or suspended.

Vandalism
Vandalism may result in restriction or cancellation of technology privileges, disciplinary action (including suspension or termination), and/or legal action. Vandalism includes any malicious or intentional attempt to harm, destroy, modify, abuse or disrupt:

- any network within the District or any network connected to the Internet,
- any form of electronic communication on any network or system,
- the data of another person,
- authorized access and use by another person,
- District software, hardware, systems or services, or
- any other system accessible by District or Personal Technology.
- deploying or using network devices and cables not pre-approved by the District's Information Technology department,
- installing or attempting to install software onto District Technology without prior authorization from the Technology Services Department and the responsible administrator(s) or in violation of software license terms and conditions,
- attempting to bypass Internet filters by means other than one's own authorized and personally-assigned override credentials,
- using applications or services that consume abnormal significant network bandwidth without prior authorization from Technology Services and the responsible administrator(s), and
- loading, creating or attempting to create computer viruses or other malware.

Reckless behavior which results in the consequences above may be regarded as vandalism.

Unauthorized software
Staff and guests are prohibited from using or possessing any software that has been downloaded or is otherwise in the user's possession without appropriate registration and payment of any fees owed to the software owner.

Local and Internet-based applications not supported by the District
To foster innovation in the use of technology in instruction, the use of local or Internet-based education applications not tested or supported by Technology Services will be permitted, under the following conditions:

- The application is purchased with District funds and its license terms are acceptable to the District's legal counsel.
- Any installation, account provisioning and support is performed either by the vendor or by authorized school or department personnel.
- The administrator of the school or department agrees to be responsible for meeting the terms and conditions required for the deployment and use of the application or service and maintains all purchase, license and deployment information needed for software audits.
- The installation, configuration or use of the application does not negatively impact District Technology and does not require intervention by Technology Services staff.

- The purchase and deployment of the application or service has prior approval from the Division of Learning Services and the acceptance of the department of Technology Services.

Learning Services or Technology Services may terminate the use of the application or service at any time should the application or service be deemed ineffective or harmful to District Technology or its users. The District is not obligated to maintain a technology environment that supports the continued use of an unsupported application.

District electronic mail (e-mail)
District e-mail is provided to staff and others for communications in support of the District's mission. Policies regarding staff use of other District Technology apply to the use of e-mail.

Since the use of e-mail is essential to the efficient and successful operation of the District, all staff are required to monitor their e-mail at least every working day. This includes days when they may be out of the office for official travel or professional development, but does not include non-contract days and absences for personal reasons such as vacation, personal time off, holidays or weekends. E-mail accounts will be maintained throughout the calendar year and e-mail may be used to disseminate information at any time.

All District e-mail users are required to maintain a standard e-mail signature block including, at a minimum, their name, title or position, and phone number.

District e-mail users shall not

- use District accounts for personal communications or encourage personal communications to be sent to these accounts,
- use a District e-mail address as an identifier for purposes not related to legitimate District activities,
- use or provide personal e-mail accounts of any type for District communications,
- give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the District unless expressly authorized to do so, or
- use e-mail in any manner that could reasonably be expected to cause strain on any computing facilities or interfere with others' use of e-mail or e-mail systems, including forwarding chain letters or sending large numbers of unsolicited or unnecessary messages.

Social media
Staff may use social media within District guidelines for instructional purposes with prior permission from Learning Services and Technology Services. As with any other instructional material, the application/platform and content shall be appropriate to the student's age, understanding and range of knowledge.

Staff may not communicate with students through personal social media platforms or by texting without prior authorization from an appropriate administrator. Staff is expected to protect the health, safety and emotional well-being of students and to preserve the integrity of the learning environment.

Staff shall not use District time or District Technology for personal use of social media. Staff shall not engage in conduct that adversely affects their capacity to serve as a role model for students or their ability to work effectively with District staff, parents, and students. Online or electronic

conduct that distracts or disrupts the learning environment or other conduct in violation of this or related district policies may form the basis for disciplinary action up to and including termination.

Assigning student projects and monitoring student use
The District will make reasonable efforts to see that the Internet and electronic communications are used responsibly by students. Administrators, teachers and staff have a professional responsibility to work together to monitor students' use of the Internet and electronic communications, help students develop the intellectual skills needed to discriminate among information sources, identify information appropriate to their age and developmental levels, and evaluate and use information to meet their educational goals.

Opportunities shall be made available on a regular basis for parents to observe student use of the Internet and electronic communications in schools.

All students shall be supervised by staff while using the Internet or electronic communications. Staff assigned to supervise student use shall have received training in Internet and electronic communications safety and monitoring student use.

Confidentiality
Staff and guests shall not access, receive, transmit or retransmit material regarding students, parents/guardians, District staff or District affairs that is protected by confidentiality laws unless such access, receipt or transmittal is in accordance with their assigned job responsibilities, applicable law and District policy. It is imperative that staff and guests who share confidential student information via electronic communications understand the appropriate use of the technology, so that confidential records are not inadvertently sent or forwarded to the wrong party. Staff and guests who use e-mail to disclose student records or other confidential student information in a manner inconsistent with applicable law and District policy may be subject to disciplinary and/or legal action.

If material is not legally protected but is of a confidential or sensitive nature, great care shall be taken to ensure that only those with a “need to know” are allowed access to the material. Staff shall handle all employee, student and District records in accordance with District policies and applicable law.

Disclosure of confidential student records, including disclosure via electronic mail or other telecommunication systems, is governed by state and federal law, including the Family Educational Rights and Privacy Act (FERPA).

Staff use of District Technology is an essential privilege, not a right
Use of the District Technology, the Internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Staff use of District Technology, the Internet and electronic communications is an essential element of employment with the District. Failure to follow the use procedures contained in this policy shall result in the loss of access to use these tools and restitution for costs associated with damages, and may result in disciplinary and/or legal action. The District may deny, revoke or suspend access to District Technology or close accounts at any time.

Staff shall be required to sign the District's Acceptable Use Agreement before network and other District Technology accounts will be issued or access allowed, and will be in force throughout the duration of employment.

School District makes no warranties
The District makes no warranties of any kind, whether express or implied, related to the use of District Technology, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement by the District of the content, nor does the District make any guarantee as to the accuracy or quality of information received. The District shall not be responsible for any damages, losses or costs a staff member or guest suffers in using the Internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via the Internet and electronic communications is at the staff member's or guest's own risk.

Adopted 6/8/99
Revised 6/14/2012
Revised 12/11/2012

LEGAL REFS.: 47 U.S.C. 254(h) (Children's Internet Protection Act of 2000)
47 U.S.C. 231 et seq. (Child Online Protection Act of 2000)
20 U.S.C. 6801 et seq. (Elementary and Secondary Education Act)
C.R.S. 22-87-101 et seq. (Children's Internet Protection Act)
C.R.S. 24-72-204.5 (monitoring electronic communications)

4813-0863-5921, v. 1