STAFF COMPUTER, E-MAIL, NETWORK, AND INTERNET USE

Purpose

The purpose of this policy is to define the proper use of computers, computer networks, messaging systems, electronic mail (e-mail) systems, Internet, or online services or wireless communication devices by staff members in the District. This policy applies not only to the use of District computers and other electronic equipment, including wireless devices, when on school grounds, but also when used by staff off of school grounds. This policy also applies to the use of staff-owned computers and wireless communication devices when using District networks. Likewise, this policy applies to the use of personally-owned computers, computer networks, messaging systems, electronic mail (e-mail) systems, or other forms of Internet access or online services or the use of any personal wireless communication device by staff members in the District during school hours while on District property or at a school sponsored event or activity.

Definition of "Wireless Communication Device"

A wireless communication device ("WCD") is an electronic device that emits an audible signal, vibrates, displays a message, or otherwise summons or delivers a communication to the possessor. The following devices are examples of WCDs: cellular and wireless telephones, pagers/beepers, personal digital assistants ("PDA"), Blackberries/smartphones, Wi-Fi-enabled or broadband access devices, two-way radios, video broadcasting devices, and other devices that allow a person to record and/or transmit, on either a real-time or delayed basis, sound, video or still images, text, or any other information. This definition does not include still or video cameras which have no communication capabilities. The District reserves the right, in its sole discretion, to determine which types of devices it will allow students to use pursuant to this policy. Such determinations are subject to change.

Policy

It is the responsibility of each employee to ensure that this technology is used for proper educational purposes and in a manner that does not compromise the confidentiality of proprietary or other sensitive information.

Coverage

This policy applies to all users of the District's computers, computer networks, messaging systems, electronic mail (e-mail) systems, Internet, or online services or District provided wireless communication devices. This policy also applies to all personally-owned computers, computer networks, messaging systems, electronic mail (e-mail) systems, or other forms of Internet access or online services or the use of any personal wireless communication device by staff members in the District during school hours while on District property or at a school sponsored event or activity.

Acceptable and Unacceptable Uses

The computers, computer network and messaging systems of the District are intended primarily for educational uses and work-related communications only. The following are uses that are unacceptable under any circumstances:

- The transmission, posting, or downloading, of any language or images which are pornographic or of a graphic sexual nature.
- The transmission of jokes, pictures, or other materials which are obscene, lewd, vulgar, or disparaging of persons based on their race, color, gender, age, religion, national origin, or sexual orientation.
- The transmission of messages or any other content which would be perceived by a reasonable person to be harassing, demeaning, threatening, disruptive or inconsistent with the Board of Education's policies concerning equal employment opportunity or sexual harassment.
- Uses that constitute defamation (libel or slander).
- Uses that violate copyright laws.
- Uses that attempt to gain unauthorized access to another computer system or to impair the operation of another computer system (for example, "hacking" and other related activities or the transmission of a computer virus or an excessively large e-mail attachment).
- Any commercial or profit-making activities.
- Any fundraising activities, unless specifically authorized by an administrator.
- Any personal use or uses which are inconsistent with the educational goals and objectives of the District.

Guidelines

Smooth operation of the Board's network relies upon users adhering to the following guidelines. The guidelines outlined below are provided so that users are aware of their responsibilities.

- Staff members must always follow the prohibition against releasing education records or personally identifiable information as set forth in FERPA and other state and federal laws regarding student privacy.

- Staff members are responsible for their behavior and communication on the Internet.

- Staff members may only access the Internet by using their assigned Internet/E-mail account. Use of another person's account/address/password is prohibited. Staff members may not allow other users to utilize their passwords.

- Staff members may not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users, or misrepresent other users on the network.

- Staff members may not upload a worm, virus, or other harmful programming or form of vandalism.

- Transmission of any material in violation of any state or federal law or regulation, or Board policy is prohibited.

- Any use of the Internet for commercial purposes, advertising, or political lobbying is prohibited.

- Staff members are expected to abide by the following generally accepted rules of network etiquette:

    - Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through the Board's computers/network. Refrain from using obscene, profane, vulgar, sexually explicit, defamatory, or abusive language in your messages.

    - Never reveal names, addresses, phone numbers, or passwords of students or other staff members while communicating on the Internet.

- Use of the Internet to access, process, distribute, display or print child pornography and other material which is obscene, objectionable, inappropriate or harmful to minors is prohibited. As such, the following material is prohibited: material that appeals to a prurient interest in nudity, sex, and excretion; material that depicts, describes or represents in a patently offensive way with respect to or what is suitable for minors an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals and material that lacks serious literary, artistic, political or scientific value as to minors. Offensive messages and pictures, inappropriate text files, or files dangerous to the integrity of the Board's computers/network (e.g., viruses) are also prohibited.

Security and Integrity

Staff members shall not take any action which would compromise the security of any computer, network or messaging system. This would include the unauthorized release or sharing of passwords and the intentional disabling of any security features of the system. Staff shall not permanently delete the District's computer files or other data without the express consent of their supervisor.

Staff members shall not take any actions which may adversely affect the integrity, functionality, or reliability of any computer (for example, the installation of hardware or software not authorized by the System Administrator).

Staff members shall report to the System Administrator or to a District Administrator any actions by students which would violate the security or integrity of any computer, network or messaging system whenever such actions become known to them in the normal course of their work duties. This shall not be construed as creating any liability for staff members for the computer-related misconduct of students.

On-Line Purchases

A staff member shall only use the network to make on-line purchases or payments for goods and services if the goods or services are being purchased by or on behalf of the District. Such purchases or payments must still have the prior authorization of the building principal or Superintendent's designee.

Right of Access

The operational and security needs of the District's computer network and messaging systems require that full access be available at all times. The District, therefore, reserves the right to access and inspect any computer, device, or electronic media within its systems and any data, information, or messages which may be contained therein. All such data, information, and messages are the property of the District.

Staff members have no privacy interest in the contents stored on or accessed through, or in the internet activity of, the computers, computer network or messaging systems of the District. The District may search files, folders, pictures, video, internet activity, internet cache, web history, keychain items, or any data stored on or accessed by the computers, computer network, or messaging systems at any time.

Standards of Behavior for All Staff Online Activity

The laws, professional expectations, and guidelines for interacting with students, parents, and other members of the District community that staff members are expected to follow also apply to their online activity. This includes participation in social media sites, such as LinkedIn, Twitter, Facebook, YouTube, and MySpace, or blogs, wikis, and other forms of user-generated media.

Staff members are personally responsible for any inappropriate or illegal content they publish on social media sites. Staff members are discouraged from "friending" current students on social networking sites unless that social network site is provided by the District, or unless the student is a family member of the staff member.

Adopted: November 19, 2018