

## **4040 Employee Use of Technology**

The Governing Board recognizes that electronic resources can enhance employee performance by improving access to and exchange of information, offering effective tools to assist in providing a quality instructional program, and facilitating District and school operations. The Board expects all employees to learn to use the available technology resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive training in the appropriate use of these resources.

Employees are responsible for the appropriate use of technology and shall use the District's Electronic Information Resources only for purposes related to their employment. Such use is a privilege that may be revoked at any time. Documents, files, and communications transmitted over electronic networks, including email and voice mail, are not private. These technologies may not be used to transmit confidential information about students, employees, or District operations without authorization.

The Superintendent or designee shall ensure that all District devices with Internet access have a technology protection measure that prevents access to visual depictions that are obscene or child pornography, or harmful to minors, and that the operation of such measures is enforced. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. (20 USC 6777; 47 USC 254)

To ensure proper use of the system, the Superintendent or designee may monitor the District's Electronic Information Resources, including email and voice mail systems, at any time without advance notice or consent. Passwords must be shared with the Superintendent or designee upon request.

The Superintendent or designee shall establish administrative regulations that describe employee obligations and responsibilities related to the use of District technology. He/she may establish guidelines and limits on the use of Electronic Information Resources. Inappropriate use will result in a cancellation of the employee's user privileges, disciplinary action and/or legal action in accordance with law, Board policy and administrative regulations.

Before using the District's Electronic Information Resources, each staff member must sign and return an *Acceptable Use Agreement* specifying user obligations and responsibilities. In that agreement, the employee agrees to not hold the District responsible and to indemnify and hold harmless the District and District personnel for the failure of any technology protection measures, violations of copyright restrictions, the user's mistakes or negligence, or any costs incurred by the user.

All staff members are directly responsible for any charges or legal violations as a result of their use of electronic information resources and liable for any damages and subject to disciplinary action.

### **Prohibited Activities**

The following on-line/Internet activities are prohibited and may result in disciplinary action:

1. Unauthorized access, including "hacking" and other unlawful on-line activities.
2. Use of electronic mail, social media, and other electronic communication forums for personal purposes.
3. Disclosure, use and dissemination of personal identification information regarding students or employees.
4. On-line conduct that would violate any applicable state or federal law.

## **4040 Employee Use of Technology (continued)**

5. On-line conduct that would violate any District policy, rule or regulation.

The Superintendent or designee shall provide copies of related policies, regulations and guidelines to all employees who use the District's Electronic Information Resources. Employees shall be asked to acknowledge annually in writing that they have read and understood these policies, regulations and guidelines.

In the event the use of an Electronic Information Resource affects the working conditions of one or more employees, the Superintendent or designee shall notify the employees' exclusive representative.

### **Use of Personally Owned Electronic Devices**

A personal electronic device is a privately owned technological device that includes laptops, tablets, netbooks, e-books, Chromebooks, flash drives, cellular telephones, or other current or emerging devices that can be used for word processing, Internet access, recording of images or sound, email, messaging, apps, or any similar electronic device.

Employees may not use personally owned electronic devices for personal business or communication while on duty, except in emergency situations or during scheduled work breaks.

Employees may use approved personally owned electronic devices for District purposes to stay connected to colleagues and the workplace, access and use work-related data, or complete tasks related to their employment. Approval to use a personally owned device for these purposes must be obtained in advance from the system administrator and the employee's site administrator or manager.

Use of personally owned electronic devices for District purposes is subject to the same rules and regulations as District-owned devices. By using a personally owned device for District purposes, the employee agrees that the District may access and monitor any District-related content on the device, and may inspect the device at any time to determine its security and appropriateness for such use.

An employee who uses a personally owned electronic device in violation of law, Board policy, administrative regulation, or the Employee Acceptable Use Agreement may be subject to discipline, up to and including dismissal, and may be referred to law enforcement officials as appropriate.

### **Social Media**

District employees who participate in official District social media platforms must adhere to all applicable policies and regulations, including but not limited to professional standards related to interactions with students, staff, and the public.

Employees should not communicate with current District students through social media sites that are personal to staff members or students, do not have an instructional or educational purpose, or do not communicate relevant information about school-related activities. Employees should be mindful about maintaining appropriate professional boundaries with students. If a student directly or indirectly communicates to a staff member about known or suspected child abuse or neglect, a threat of harm to the student or others, or evidence of a crime, the staff member must immediately notify the appropriate authorities and the site administrator or designee.

Use of official District social media platforms in violation of this administrative regulation may result in disciplinary action, up to and including dismissal from employment. The District may suspend or revoke user privileges of individuals who violate District standards on social media.

## **4040 Employee Use of Technology (continued)**

**Board Approved:**

October 10, 2018

July 22, 2015

August 19, 2004

Effective Date: August 19, 2004