## Policy 4040: Employee Use Of Technology

**Status:** ADOPTED

**Original Adopted Date:** 07/15/2009 | **Last Revised Date:** 01/19/2017 | **Last Reviewed Date:** 01/19/2017

The Board of Trustees recognizes that technological resources can enhance employee performance by offering effective tools to assist in providing a quality instructional program, facilitating communications with parents/guardians, students, and the community, supporting district and school operations, and improving access to and exchange of information. The Board expects all employees to learn to use the available technological resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive professional development in the appropriate use of these resources.

Employees shall be responsible for the appropriate use of technology and shall use the district's technological resources primarily for purposes related to their employment.

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

The Superintendent or designee shall establish an Acceptable Use Agreement which outline employee obligations and responsibilities related to the use of district technology. Upon employment and whenever significant changes are made to the district's Acceptable Use Agreement, employees shall be required to acknowledge in writing that they have read and agreed to the Acceptable Use Agreement.

Employees shall not use district technology to access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, sexually explicit, or unethical or that promotes any activity prohibited by law, Board policy, or administrative regulations.

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that prevents access to visual depictions that are obscene or child pornography 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)

In addition, employees shall be notified that records maintained on any personal device or messages sent or received on a personal device that is being used to conduct district business may be subject to disclosure, pursuant to a subpoena or other lawful request.

Employees shall report any security problem or misuse of district technology to the Superintendent or designee.

Inappropriate use of district technology may result in a cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law, board policy, and administrative regulation.

Employees should have no expectation that any communications made using the District's information and communication systems and equipment are exempt from monitoring or access by the District.

**Public Records and Retention**

1. Information stored on the District's system and equipment, including email, email attachments, Web postings, and voice mail messages may become records of the District. District records pertaining to the District's business, whether stored in hard copy or electronically, may be considered public records and, therefore, subject to the Public Records Act ("PRA") and Title 5, section 16020, et seq., of the California Code of Regulations, pertaining to the retention and destruction of school records.

2. A District email account is not intended for permanent storage of email. It is each employee's responsibility to save and/or file email that he or she wishes to access, or that are District records and required to be retained

by law. "District records" means all records, maps, books, papers, and documents prepared or retained as necessary or convenient to the discharge of official duty and includes any writing containing information related to the conduct of the public's business prepared, School District Email Retention owned, used, or retained by the District regardless of physical characteristics. District records shall be either: (1) saved to an electronic system other than the District email account, (2) electronically archived, or (3) printed on paper and filed as appropriate. Email and other electronic files that are classified pursuant to the District's administrative regulation regarding retention of documents - AR 3580 shall be preserved in one of the three manners described above.

3. The District may access and, to the extent required or allowed by law, disclose any email received, sent, or stored in a District email account. The District may retain or dispose of an employee's email, whether an employee is currently or formerly employed by the District. Email account in-boxes and out-boxes may be purged of email older than five years by the District's information technology department. Email trash folders may be purged as often as every 30 days by the District's information technology department. Staff must notify superintendent or designee of litigation or anticipated litigation in order to preserve related electronic communication.

---