EMPLOYEE USE OF TECHNOLOGY

Online/Internet Services: User Obligations and Responsibilities

Employees are authorized to use district equipment to access the Internet or other online services in accordance with Board of Trustees policy, user obligations and responsibilities specified below.

1. The employee in whose name an online services account is issued is responsible for its proper use at all times. Employees shall keep account information, home addresses, and telephone numbers private. They shall use the system only under their own user account.

2. Employees shall use the system, responsibly and primarily for work-related purposes. Use of district resources and equipment for commercial, illegal, or political use is strictly prohibited. The district has the right to monitor its computer technology and networks for improper, inappropriate and /or unauthorized use.

3. Employees shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability, religion, or political and cultural beliefs.

(cf. 4030 - Nondiscrimination in Employment)
(cf. 4119.11/4219.11/4319.11 - Sexual Harassment)

4. Employees shall not use the system to promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.

(cf. 4119.25/4219.25/4319.25 - Political Activities of Employees)

5. Copyrighted material may not be placed on the system without the author's permission. Employees may download copyrighted material only in accordance with applicable copyright laws.

(cf. 6162.6 – Use of Copyrighted Materials)

Employees shall not invade the privacy of others by attempting to access other users' accounts or by releasing others' personal information. Employees shall not attempt to interfere with other user's ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or forge other users' email, files or data.

Employees shall not intentionally upload, download or create computer viruses and/or maliciously attempt to harm or destroy district equipment or materials or the data of any other user, including so-called "hacking."

Employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the district or using district equipment or resources without permission of the Superintendent or designee. Such sites shall be subject to rules and guidelines established for district online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs, any such site shall include a disclaimer that the district is not responsible for the content of the messages. The district retains the right to delete material on any such online communication.

Users shall report any security problem or misuse of the services to the Superintendent or designee.

(*cf. 6163.4* – Student use of Technology)

10. No one shall provide access to the district's Internet to unauthorized individuals without prior consent from the Superintendent, principal or their designee(s).

11. Vandalism, attempted otherwise, will result in the immediate cancellation of user privileges in addition to fines, disciplinary actions and possible criminal or civil prosecution. Vandalism includes, but is not limited to, hacking into computer technology and/or networks, attempting to gain access or gaining access to student records, grades or files, transmitting of viruses, "Trojan Horses," or any hardware, software, data, or network performance.

12. Employees shall not purposefully use district technology equipment to produce or distribute multiple copies of messages, documents, or files in a manner which is illegal or cause degradation or damage to its hardware, software, data, or file network performance.

13. Employees shall not attempt to impersonate or represent another person, nor may employees use the district's name, the name of district school sites or other facilities, or district or school logos or symbols without prior approval from the Superintendent or designee. The district reserves the right to control the unauthorized use of its names, symbols, logos, or any other proprietary materials to the extent permitted by law.

14. Employees may not use or alter any passwords, recognition codes, security devices or methods, data encryption, or physical locking devices, such as locks on any part of the district's computer technology and/or network, without the district's written consent.

15. Employees many encounter material they interpret as controversial, inappropriate, or offensive. The district has implemented filtering and/or blocking software to restrict access to Internet sites containing pornography, or other obscene depictions. It is the responsibility of the Employee not to intentionally search for or access such material. Employees agree to hold the district and Board Members and agents harmless in the event the Employee obtains access to controversial or inappropriate materials while using the computer technology and/or network.

16. Employees are prohibited from using district computer technology or network to engage in activities that would subject the district, school or individual to criminal, civil or administrative liability.

17. Employees shall not obtain, send or access information which could be used to make destructive devices such as guns, weapons, bombs, explosives, or fireworks.

18. Employees are responsible for any losses sustained by the district or its affiliates, resulting from their intentional misuse of the district's computer technology or network.

19. Employees with district email accounts are to check their email frequently and delete unwanted messages and other files of data that take up excessive storage space. The system administrator may delete old messages from user accounts should the need arise.

Public Records and Retention

20. 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 to the extent required by the law, 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 to serve as a 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, owned, used, or retained by the District regardless of physical characteristics. Email and other electronic files that are classified as Class 1 or Class 2 records pursuant to AR 3580 shall be preserved in one of the three manners described in AR 3580.

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 as often as once a year by the District's information technology department. Email trash folders may be purged as often as 90 days by the District's information technology department.