COMPUTER SECURITY, E-MAIL, AND INTERNET
COMMUNICATIONS POLICY

The District has established this policy with regard to access and disclosure of electronic data composed, stored, sent, or received by employees using the District computer system. This policy is designed to protect the safety and security of the District's computer systems, including E-mail and Internet use.

The District intends to enforce the rules set forth below and reserves the right to change these rules at any time.

1. The computer hardware system, software, and E-mail system are owned by the District, and all messages or data composed, stored, sent, or received using the system are and remain the private property of the District. These are not the property of the employee.

2. The computer and E-mail systems are to be used for business purposes only. Personal business is unauthorized and should not be conducted on the system.

3. The electronic mail system may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

4. The District prohibits discriminatory, harassing, or offensive materials in any form of media. Among those that are considered offensive are any messages that contain sexual implications, racial slurs, gender-specific comments, or any other comments that offensively address someone's age, sexual orientation, religious or political beliefs, national origin, or disability.

5. The electronic mail system shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

6. The District reserves, and intends to exercise without prior notice, the right to read, review, audit, intercept, access, or disclose any and all information on an employee's computer system or messages created, received, or sent over the electronic mail system for any purpose, even if coded or passworded.

7. The confidentiality of any message or data should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. The use of passwords for security does not guarantee confidentiality, or that the District will not retrieve it. All passwords must be disclosed to the computer administrator.

COMPUTER SECURITY, E-MAIL, AND INTERNET
COMMUNICATIONS POLICY
(continued)

8. Any communications created, sent, or retrieved using E-mail may be read by individuals other than the intended recipient.

9. Notwithstanding the District's right to retrieve and monitor any E-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any E-mail that is not sent to them. Any exception to this policy must receive prior approval by the Superintendent.

10. Any employee who violates this policy or uses the computer system or electronic mail system for improper purposes shall be subject to discipline up to and including discharge.

11. The District has the authority to terminate or limit access to any program at any time.

12. Personal storage devices may contain viruses with the potential to harm our system. Use of these devices is strongly discouraged. It is strongly recommended that Google apps be used for sharing files.

13. The District will take all necessary measures to maintain student privacy relative to the District's website, online information, and storage of student personally identifiable information, as required by state and federal law.

Adopted: May 16, 2002
Revised: February 17, 2016