POLICY TITLE: Internet, Email and Electronic Communications
POLICY NUMBER: 3300

3300.1 The District believes that employee access to and use of the internet, email, and other electronic communications resources, benefits the District and makes it a more successful local public agency. However, the misuses of these resources have the potential to harm the District's short and long-term success. Employees should have no expectation of privacy in work-related emails or internet usage while using District computers.

The District has established this policy to ensure that the District employees use the District-provided computer resources, such as the internet and email, in an appropriate manner.

3300.2 Rules Regarding Prohibited Use

Employees shall not use the District internet and email in an inappropriate manner. Prohibited use of the internet and email systems includes, but is not limited to:

a) Accessing internet sites that are generally regarded in the community as offensive (e.g., sites containing pornography or that exploit children), or accessing sites for which there is no official business purpose (e.g., social media websites or online shopping websites).
b) Engaging in any profane, defamatory, harassing, illegal, discriminatory, or offensive conduct or any conduct that is otherwise inconsistent in any way with the District policies.
c) Distributing copyrighted materials.
d) As computer viruses can become attached to executable files and program files, receiving or downloading executable files and programs via email or the internet without express permission of the Systems Administrator is prohibited. This includes, but is not limited to, software programs and software upgrades. This does not include email or documents received via email and the internet.
e) Use of another person's name or account, without express permission of the System Administrator, is strictly prohibited.
f) Using the District's computer resources for personal social media, online shopping, and other similar online commercial activity.
g) Employees must respect all copyright and licensed agreements regarding software or publication they access or download from the internet. The District does not condone violations of copyright laws and licenses and the employee will be personally liable for any fines or sanctions caused by the employee's license or copyright infringement.

3300.3 Additional Guidelines

Employees are expected to understand and comply with the following additional guidelines regarding use of the internet and District computer systems.

a) Internet access is to be used for the District business purposes only. Employees who have completed all job tasks should seek additional work assignments. Use of the internet should not interfere with the

timely and efficient performance of job duties. Personal access to the internet and email is not a benefit of employment with the District. Limited personal use of the District's systems to access internet, email, and other electronic communications may be permitted only during the employees' authorized break time.

b) Employees do not have any right or expectation to privacy in any of the District computer resources, including email messages produced, sent, or received on the District computers or transmitted via the District's servers and network. The District may monitor the contents of all computer files and email messages to promote the administration of the District operations and policies.
c) Employees' access to and use of the internet, email, and other electronic communications on the District systems is monitored, and such files and electronic communications may be reviewed by the District at any time. Employees have no expectation of privacy.
d) Deleting an email message does not necessarily mean the message cannot be retrieved from the District's computer system. Backup copies of all documents, including email messages, that are produced, sent, and received on the District's computer system, can be made.
e) Email and any attachments are subject to the same ethical standards, and standards of good conduct, as are memos, letters, and other paper-based documents.
f) Currently all District email sent is not encrypted. Unencrypted email is not a secure way of exchanging information or files. Accordingly, employees are cautioned against transmitting information in an email message that should not be written in a letter, memorandum, or document available to the public.
g) Email, once transmitted, can be printed, forwarded, and disclosed by the receiving party without the consent of the sender. Use caution in addressing messages to ensure that messages are not inadvertently sent to the wrong person.
h) Virus scanning software shall be used where provided.
i) It is advisable for all employees of the District to remind customers, clients, and contractors of security issues when sending confidential email or documents to the District via email. If applicable, our customer, clients, or contractors should be reminded to implement a security policy and make sure their employees understand the ramifications of sending confidential information via email.
j) Employees must scan all downloadable materials before using or opening them on their computers to prevent the introduction of any computer virus.