# Los Osos Community Services District

## Internet, Email and Electronic Communications Policy

PURPOSE

The Los Osos Community Services District (hereinafter "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.

POLICY

E-mail is a business tool which is to be used in accordance with generally accepted business practices and current law reflected in the California Public Records Act to provide an efficient and effective means of communications for the District.

The District respects the individual privacy of its employees. However, an employee cannot expect privacy rights to extend to work-related conduct or the use of District-owned equipment or supplies. Consequently, E-mail users shall have no reasonable expectation of privacy in E-mail communications sent over the System as E-mail communications are not confidential.

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.

   1. 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.

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.

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.

REPORTING ISSUES TO IT

Even with every possible protection in place, a security breach is still a possibility. The best way to mitigate the impact of this is to recognize the signs of a breach, and report it to IT immediately so they can investigate and take any necessary steps. Workers should be aware of:

A. A sudden increase in pop up ads and spam.

B. A significant decrease in performance.

C. Frequent error messages.

D. A new homepage or default search engine.

E. Anti-malware software indicating that a virus or malware is present.

F. Never share sensitive information with an unauthorized party. This may sound obvious but all too often employees feel some sort of social pressure when someone else asks them for information (this applies to people within your organization too). If there's any doubt, say no and consult a supervisor for permission.

G. Be careful about what you share on social media. Whether you are on a personal or work account, criminals can gain insights from sensitive data you share that can help them target you.

H. Slow down and evaluate emails carefully before clicking or taking action.

I. Never click links from an unknown sender before carefully vetting the URL. They may pose as someone from your company or a reputable company, use a URL similar to a well-known site, use logos and disguised email accounts — pay close attention to detail.

J. Keep an eye out for strange requests, spelling and grammar mistakes, flashy click-bait content and other things that may seem "off."

It's imperative that workers contact IT if they realize that someone may have gained unauthorized access via social engineering. This is a common method where someone posing as a support agent or other authority talks someone into providing access to their devices, usually using some sort of screen sharing software.