RANCHO MURIETA COMMUNITY SERVICES DISTRICT

Category:	Personnel	**Policy #** 2003-3
Title:	Internet, E-mail, and Electronics Communication Ethics, Usage and Security Policy	

PURPOSE

The District has established this ethics, usage, and security policy to ensure that all District employees use the computer resources, which the District has provided its employees, such as the Internet and e-mail, in an ethical, legal, and appropriate manner. This policy establishes what is acceptable and unacceptable use of the Internet, e-mail, and other electronic communications.

This policy also establishes the steps the District may take for inappropriate use of the Internet and e-mail. All employees must read and adhere to the guidelines and policies established herein. Failure to follow this policy may lead to discipline, up to and including immediate termination.

BASIC POLICY AND OBJECTIVES

The Rancho Murieta Community Services District believes that employee access to and use of the Internet, e-mail, and other electronic communications resources benefits the District and makes it a more efficient and successful local public agency. However, the misuses of these resources have the potential to harm the District's short and long-term success.

1) Employees shall not use the Internet or e-mail in an inappropriate manner. Inappropriate use of the internet and e-mail includes, but is not limited to:

   a) Accessing internet sites that contain pornography, exploits children, or sites that would generally be regarded in the community as offensive, or for which there is no official business purpose to access.

   b) Participating in any profane, defamatory, harassing, illegal, discriminatory, or offensive activity or any activity that is inconsistent in any way with the District's policies (i.e. policy on sexual harassment).

   c) Exploiting security weaknesses of the District's computing resources and/or other networks or computers outside the District.

   d) Internet access and e-mail usage is to be used for District business purposes only (unless the employee is on break). 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. Access to the Internet and e-mail is not a benefit of employment with the District.

2) Employees do not have any right to privacy in any District computer resources, including e-mail messages produced, sent, or received by District computers or transmitted via the District's servers and network. Employee access to the Internet and e-mail is controlled by use of a password. The existence of a password does not mean that employees should have any expectation of privacy. Employees must disclose their passwords to the District upon request, and the District will maintain a file of all passwords currently in use. The District may monitor the contents of all e-mail messages to promote the administration of the District, its business, and policies.

3) Employees access to and use of the Internet, e-mail, and other electronic communications will be monitored frequently. Failure to follow the policy may lead to discipline, up to and including immediate termination. Disciplinary action may include the removal of Internet and e-mail access from their computer or termination of employment with the District.

4) The Internet and e-mail provide means by which employees of the District may communicate with its customers (general public). Messages to or from customers through the District's e-mail system may be considered part of the District's business records and should be treated as such.

5) Deleting an e-mail message does not necessarily mean the message cannot be retrieved from the District's computer system. For a specific period of time, the District retains backup copies of all documents, including e-mail messages, produced, sent, and received on the District's computer system.

6) E-mail and any attachments are subject to the same ethical and legal concerns and standards of good conduct as memos, letters, and other paper-based documents. E-mail can be forwarded to others, printed on paper, and is subject to possible discovery during lawsuits in which the District may be involved.

7) Currently all District e-mail being sent is not encrypted. Unencrypted electronic mail is not a secure way of exchanging information or files. Due to the way Internet data is routed, all messages are subject to "eavesdropping." Messages may be "stolen" as they temporarily reside on host machines waiting to be routed to their destination, or they may be purposefully intercepted from the Internet during transfer to the recipient. It is possible for someone other than the intended recipient to capture, store, read, alter/or re-distribute your message. Do not transmit information in an electronic mail message that should not be written in a letter, memorandum, or document available to the public.

8) E-mail, 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.

9) Use of electronic mail or the Internet to distribute copyrighted materials is prohibited.

10) Each user should take the necessary steps to prevent unauthorized disclosure of confidential or privileged information. (This is especially important for law firms and accounting firms that have strict professional ethical obligations and duties toward their clients.)

11) Use of electronic mail or the Internet to send offensive messages of any kind is prohibited.

12) Use of electronic mail or the Internet for inappropriate or unauthorized advertising and promotion of the District is prohibited.

13) When District employees communicate using electronic mail or other features of the Internet, the employee must be extremely mindful of the image being portrayed of the District.

14) Computer viruses can become attached to executable files and program files. Receiving and/or downloading executable files and programs via electronic mail or the Internet without express permission of the Director of Administration/Systems Administrator is prohibited. This includes, but is not limited to, software programs and software upgrades. This does not include e-mail and/or documents received via e-mail and the Internet. All downloaded files must be scanned for viruses.

15) Use of another user's name/account, without express permission of the Director of Administration/Systems Administrator, to access the Internet is strictly prohibited.

16) Personal use of the District's computer resources for personal commercial activity or any type of illegal activity is strictly prohibited.

17) It is advisable for all employees of the District to remind customers/clients/contractors of these security issues when sending confidential electronic mail and/or documents to the District via electronic mail. If applicable, our customer/clients/contracts should be reminded to implement a security policy and make sure their employees understand the ramifications of sending privileged information via electronic mail. (This is especially important for law firms and accounting firms that have strict professional ethical obligations and duties toward their clients.)

18) The District will not be responsible for maintaining or payment of personal Internet accounts or related software.

19) E-mail that users need to retrieve from their personal Internet account must be retrieved via that User's personal Internet account. District users shall not access such personal e-mail account using the District's network system, telephone system, modems, or communication server.

20) Employees will only access the Internet through the District's network. Internet access through other methods (i.e. modems) will not be allowed, unless specifically authorized by the Director of Administration/Systems Administrator.

21) Employees will only access the Internet using the approved Internet browser (Internet Explorer). Any other browser being used on a workstation will be promptly removed.

22) Employees will respect all copyright and license agreements regarding software or publication they access or download from the Internet. The District will not condone violations of copyright laws and licenses and the employee will be personally liable for any fines or sanctions caused by the license or copyright infringement. Any software or publication, which is downloaded onto District computer resources, becomes the sole property of the District and must have prior approval from the Director of Administration/Systems Administrator.

23) Employees will only download information and/or publications for official business purposes.

24) Employees are to scan all downloaded materials before using or opening them on District computers to prevent the introduction of computer viruses.

25) All list subscriptions should be for business purposes only. The employee will make sure List Servers are notified when the employee leaves the District.

Employee Acceptance. By signing this agreement, I hereby represent that I have read, understand, and agree to the District's Internet, e-mail, and electronic communications ethics, usage, and security policy.

Date

Signature

Print name here

Approved by CSD Board of Directors	February 12, 2003