Board of Directors Approved on June 19, 2003

POLICY TITLE: Internet and E-mail Policy

POLICY NUMBER: 3300

I. PURPOSE

The Cambria Community Services District's ("District") computer systems, including all hardware and software, are the exclusive property of the District and are provided for creating and transmitting business-related information. The District treats all computer files, including electronic mail (e-mail), whether sent or received, as business information. The purpose of this policy is to:

- Ensure that the computer systems are used for appropriate District business;
- Notify employees that they have no right to privacy in the use of the computer systems, including e-mail or Internet; and
- Notify employee that the District reserves the right, with or without notice, to access, monitor, review, copy and/or delete any computer files, including e-mail sent or received, and all website communications and transactions.

II. E-MAIL USE

A. All e-mail business communications to non-District employees should use an appropriate professional tone, correct spelling, and proper grammar.
B. The District reserves the rights to access, monitor, copy and/or delete any e-mail communications made on the District computer systems.
C. There should be no expectation of privacy in the use of e-mail. Employee should not use District e-mail facilities to create or transmit information they wish to keep private.
D. When transmitting messages via e-mail, employees should be aware that e-mail messages can be read by persons other than the addressee, and that messages may be later disclosed to outside parties. E-mail messages, including but not limited to, information relative to public projects or policy decisions may be subject to disclosure under the California Public Records Act (Government Code Section 6250 et seq.). E-mail messages may also be subject to disclosure in litigation or administrative proceedings in the same manner as other District records.
E. E-mail messages sent to and received from attorneys representing the District are privileged communications. Such e-mail communications shall not be distributed or copied to unauthorized individuals.

III. INTERNET USE

A. Employees may not access or otherwise use the Internet while on duty without the express permission of the District General Manager or his/her designated representative, except infrequent incidental personal use that does not adversely affect the ability to perform work duties. Internet access shall be limited to work related sites during workday hours.

B. Employees have no right to privacy in the use of the Internet on District computer systems.
C. The District reserves the right, with or without notice, to access, monitor, review, copy and/or delete any computer files, including any and all website communications and/or transactions by District employees. The District further reserves the right to monitor any employee's Internet use for the purposes of determining whether such use is appropriate or acceptable.

IV. PROHIBITED USES OF E-MAIL AND THE INTERNET

Prohibited uses of e-mail and/or the Internet on District computer systems include, but are not limited to, the following:

A. To access any obscene, pornographic, or materials that are in poor taste;
B. To transmit sexually explicit images, messages, and/or cartoons; ethnic or racial slurs, or anything that may be construed as harassment or disparaging of others based on their race, national origin, ethnic group identification, religion, age, sex, sexual orientation, marital status, color or physical or mental disability;
C. To conduct on-going personal business or family business;
D. To play games;
E. To conduct illegal activities, such as, but not limited to, gambling, or commit a crime or fraud, or violate any federal, state or local law;
F. To use the user-name or password of another person to gain access to his/her e-mail or any other computer file or account without that person's permission;
G. To transmit sensitive or privileged information to unauthorized persons or organizations;
H. To download or otherwise acquire software without prior consent of the District General Manager, or his/her designee; and
I. To use the Internet in any manner that causes confidential or sensitive information to be subject to eavesdropping or interception by unauthorized individuals.

V. COMPUTER SYSTEMS – HARDWARE AND SOFTWARE

Prohibited activities with regard to employee use of District computer systems—hardware and software—include, but are not limited to, the following:

A. Installing programs on District computer systems without prior consent of the District General Manager, or his/her designee;
B. Copying any District computer program for the purpose of using it on any other computer without the prior consent of the District General Manager, or his/her designee;
C. Connecting computers, including laptops and personal computers not owned by the District, to the District's information systems network without prior written consent of the District General Manager, or his/her designee;
D. Disclosing an employee's account or e-mail password, or otherwise making such account available to others;
E. Infringing on other employee's access and use of District computer systems, including, but not limited to:
    1. Sending excessive messages, either locally or offsite;
    2. Unauthorized modification of system facilities, operating systems, or disk partitions;
    3. Attempting to crash or tie up a computer or network;
    4. Damaging or vandalizing District computing facilities, equipment, software, or computer files;

5. Intentionally using or developing programs that disrupt other computer users or which access private or restricted portions of the system and/or damage the software or hardware components of the system; or
6. Introducing or allowing the spread of any virus or destructive information, file, or other item.

VI. VIOLATION OF POLICY

Any violation of this policy, or other inappropriate use of the District's computer systems, including e-mail and Internet activities, is considered a serious violation of District policies and may result in disciplinary action, up to and including termination of employment.