POLICY TITLE: District Electronic Resources Policy and Procedures
POLICY NUMBER: 2205

The Christian Valley Park Community Services District ("District") makes every effort to provide its employees with technology resources to conduct business more effectively. The District has installed personal computers, local area networks (LANs), electronic mail (email), cell phones and access to the Internet. The purpose of the District's Electronic Resources Policy and Procedures is to establish uniform guidelines for use of this technology, including the use of the Internet and email.

Policy

2205.1 District technology, including computers, fax machines, and internet licenses are provided for District business and are not to be used for personal gain, private purposes (except as described in subsection 2205.6), or to support or advocate non-District-related business or purposes. All data and electronic messages, including information accessed via the Internet and sent or received through electronic mail (email) systems, are the property of the District. All records whether paper or electronic, may be subject to disclosure under the California Public Records Act and are not private. Notwithstanding the foregoing, email should only be used for the transmission of information and should not be used for preserving information for future reference. Information to be retained may be stored electronically on the system/network and/or may be converted to a hard copy and archived in a District physical file cabinet.

2205.2 There is no expectation of personal privacy in any use of District computer systems and software, including email and the Internet. The District may, at any time, review the contents of all records, data and communication transmitted, received and stored by its electronic systems. This review may include accessing and disclosing all electronic documents, information and messages including email and Internet records.

2205.3 The District purchases, owns and administers the necessary software and licenses and cell phones to provide access to email and Internet services and voice communications in the office, in the field and for emergency communications. Users may not rent, copy or loan District software or its documentation, nor use alternative software to access District systems. Users may be subject to discipline for negligence for introducing unauthorized software or viruses into District systems whether or not damage arises from that conduct.

2205.4 The District is not responsible for items originating from the Internet and reserves the right to restrict employee access to the Internet or to certain Internet content.

2205.5 Examples of prohibited uses:

a) Using the Internet to view, obtain or disseminate any sexually oriented material, images or messages.
b) Using the Internet and/or email systems to send or distribute disruptive, offensive, abusive, threatening, slanderous, racial or sexually harassing materials.
c) Using District computer systems for private purposes, personal gain, solicitation of commercial ventures, religious or political causes, chain letters, or other non-job-related purposes (except as described in subsection 2205.6 below).
d) Downloading or installation of software that has not been approved by the District and scanned

for viruses.

e) Sending unencrypted confidential documents via the Internet without direction from District management to do so in the course of District business.
f) Any other use that may compromise the integrity of the District and its business in any way.
g) A good rule of thumb when using the computer and email is "never put anything in an email that you would not want to see on the front page of the newspaper."

2205.6 To promote employee computer and Internet proficiency and as an employee benefit, certain incidental employee personal use is allowed. This use is only permitted during employee personal time. Examples include educational enhancement and personal communications, which conform to the above prohibited uses. Personal use is secondary, and should not (i) interfere with the agency's operation of Electronic Communications Resources, (ii) interfere with the user's employment or other obligations to the District, or (iii) burden the District with noticeable incremental costs. The District reserves the right to limit or discontinue incidental personal use of its technology resources at any time. More than occasional and incidental personal use of District re- sources is forbidden by State law.

2205.7 The acquisition of hardware and software shall follow the normal budgetary and purchasing procedures, ensuring budget authorization is in place. Requests for acquiring hardware and software shall be recommended to the General Manager for evaluation and recommendation to the Board of Directors.

2205.8 Equipment operation and maintenance:

a) The authorized technology staff (in-house or agreement/contract) shall assist in evaluating District functional needs and recommend appropriate options for improvement of District technology resources.
b) Technology staff shall maintain an on-site office automation library of proven and reliable software and hardware requiring minimum technical support that is easy to use, enhances District productivity, and is compatible with District technology systems.
c) Technology staff shall maintain an on-site inventory control of all workstation hardware and software.
d) Technology staff shall provide on-site training and consulting advice on approved software and make recommendations as appropriate.
e) Technology staff shall maintain the District technology systems including all personal computer work- stations and client server network for the purpose of retrieving data files, sharing licensed applications and nightly data backup.
f) Technology staff shall periodically review the District technology systems for adherence to operating standards and implement approved upgrades.
g) Technology staff shall backup District databases daily, weekly, monthly, quarterly and annually for archival and retrieval purposes.

2205.9 Security: The General Manager and designee must approve remote access to District systems. All computer systems users are responsible for data residing on personal devices used to access District systems remotely. Employees may not access systems remotely so as to incur overtime compensation without advance authorization by District management.

Procedures:

2205.10 Passwords:

a) Users dealing in confidential matters will define their own confidential password. Users should be aware that this does not imply that the system may be used for personal communication or that email is confidential or the property of the user.
b) To ensure the security of the email system, the system will prompt users to routinely change their pass- words. Should a user forget his or her password, the system may lock them out after three failed at- tempts.

2205.11 Internet and email access:

a) Access to the Internet and email is restricted to authorized employees. The District may deny or restrict Internet and/or email access to any employee at any time.
b) When using email and the Internet, employees are cautioned to remember they represent the District and must act professionally, courteously and so as to not bring an employee or the District into disrepute. Employees may not speak for the District unless they are authorized to do so.
c) Email and Internet messages can be forwarded without the express permission of the original author. Users must use caution in the transmission and dissemination of messages outside the District and must comply with all State and Federal laws, rules and regulations and District policy.

2205.12 Electronic Document, Software and Mail Storage

a) Electronic mail is backed-up on a regular basis. It is synchronized with the server on every start-up and shutdown. The District back-up procedures allow the District to restore current software, documents and electronic mail upon a system failure.
b) Electronic mail is not intended to be a permanent storage medium. Electronic in-boxes and out-boxes should be regularly archived or purged. The District may, in its discretion, automatically purge older mail.
c) To save critical electronic mail as a permanent record, employees should print out a hard copy for permanent filing or save the file on the “C” drive of the desktop or laptop computer assigned to them or to another electronic archive designated by District management.
d) Signature Block: Email sent outside the District should include a signature block at the end of all messages. The block should include the sender’s name, title, district name, direct telephone number, FAX number and email address and be in a format approved by District management.