POLICY 3040: Computer/Communication Hardware and Software

3040.10 Employees must use Carmichael Water District's (District) computer/communication device resources in an ethical manner with attention to:

a. Legal use of licensed software;

b. Protection of confidential information;

c. Legitimate use of hardware, software, periphery devices;

d. Legitimate access to and use of work-related data;

e. Asset management;

f. Right to privacy; and,

g. Respect for and safeguarding of security passwords, user identity, and system access.

3040.20 All material stored on any District computer, file server, communication device, or other storage media is District property. No employee may install personal software on a District computer, file server, or communication device without proper authorization. All software must be appropriately licensed. Improper use of computing resources by an employee is a violation of this policy.

3040.20.1 The following list is a sample of the types of uses that may be considered improper for any employee.

a. Use of another's login ID.

b. Frivolous use of any workstation, computer, or network device (e.g. playing games or using the internet for personal reasons during work hours).

c. Inspection of data that is neither allotted to that employee, nor specified as public.

d. Inspection of data concerning utilization, authorization, or security.

e. Modification of data that is not specifically created by or assigned to that employee.

f. Interference with other persons accessing the systems, networks, or equipment.

g. An attempt to gain access to another's resources, program(s), or data.

h. Use of another's program(s) or data without authorization.

i. Sending obscene or vulgar messages or pictures. (Note: A message may be considered to be obscene or vulgar if it is sexually explicit, lewd, indecent, crude, offensive, or unprofessional.).
j. Abuse or destruction of hardware, software, or District data.

k. Use of facilities for personal or corporate gain (e.g. the unauthorized sale or transfer of computer programs or results developed under an internal login ID).

3040.30 All electronic communications, including all software, databases, hardware, and digital files, remain the sole property of the District and are to be used only for District business and not for any personal use. Electronic communication and media may not be used in any manner that would be discriminatory, harassing, or obscene, or for any other purpose that is illegal, against District policy, or not in the best interest of the District.

3040.40 It is a violation of this policy for employees to misuse electronic communications and engage in defamation, copyright or trademark infringement, misappropriation of trade secrets, discrimination, harassment, or related actions.

3040.50 All electronic information created by any employee using any means of electronic communication is the property of the District and remains the property of the District. Personal passwords may be used for purposes of security, but the use of a personal password does not affect the District's ownership of the electronic information.

3040.60 The District reserves the right to access and review electronic files, messages, mail, and other digital archives, and to monitor the use of electronic communications as necessary to ensure that no misuse or violation of District policy or any law occurs. Employees understand that they shall have no privacy rights when using District computer systems or communication devices.

3040.70 Electronic mail ("email") is provided to some employees and at District expense to help employees carry out the District's business. The District treats all messages sent, received, or stored on e-mail as business messages and as its property. As such, the District reserves the right to assess, review, copy, or delete all e-mail messages, and to disclose them to authorized persons, inside or outside the District, as it deems appropriate. Employees may not access another employee's e-mail file.

3040.80 Hardware Usage

3040.80.1 Notebook/Laptop Computer and Communication Equipment Responsibilities: District employees are responsible for ensuring that all notebook/laptop computers and/or communication equipment are locked and secured at all times during their possession or when placed in the vehicle mount within their delegated vehicle. When a notebook/laptop computer and/or communication equipment is placed in a vehicle, that vehicle and its contents must be secured from theft and damage by rolling up all windows and locking all doors while vehicle is vacant.

3040.80.2 It is the employee's responsibility to take appropriate precautions to prevent damage to or loss/theft of the notebook/laptop computer and/or communication equipment. The employee may be responsible for certain costs to repair or replace the device if the damage or loss is due to negligence or intentional misconduct. Repair/replacement costs will be at the General Manager's discretion. Negligence or intentional misconduct of District computer and communication equipment resulting in damage is a

violation of this policy. If the notebook/laptop computer and/or communication equipment is lost or stolen it must be reported to the employee's supervisor immediately.

3040.80.3 Notebook/laptop computers and/or communication equipment should never be left unattended. Employees may not tamper with computer hardware and/or software in any way. Employees shall not have food or beverages in, on, or around the notebook/laptop computers and/or communication equipment at any time.

3040.80.4 District employees who install or use copied software without a proper license on District equipment, or who install or use software improperly copied from a District computer at home for personal, non-District use are in violation of this policy.

3040.80.5 Notebook/Laptop Computer and Communication Equipment Use: All notebook/laptop computers and/or communication equipment are intended for District related business only. If it is determined through an audit the employee has used the device for non-District purposes or has explicit pictures and/or information stored in the unit, such actions is a violation of this policy.

3040.90 Cell Phones and Other Communication Devices

3040.90.1 In accordance with California law, employees are prohibited from driving a motor vehicle on District business while holding and operating a handheld wireless telephone or an electronic wireless communication device unless the wireless telephone or electronic communication device is specifically designed and configured to allow voice-operated and hands-free operation, and it is used in that manner while driving.

3040.90.2 Telephones installed in District offices and cellular phones provided to District employees are for business purposes only. They may not be used for long-distance personal calls, except where otherwise authorized by District management.

3040.90.3 Personal calls, whether on a District or personal phone, during work hours must be kept to a minimum and should be made during breaks or meal periods.

3040.100 Social Media Policy

3040.100.1 Social media is the term for internet based tools used for publishing, sharing and discussing information. This includes blogs, wikis, and social networking sites such as Facebook, Twitter, Flickr, LinkedIn, etc. Employees might use social media as either the representative of the District making official comments or in their private capacity as a citizen. Use of the District's computer resources for connecting to, posting on, or reviewing correspondences to or from social media will adhere to the guidelines previously outlined in this policy as well as the following:

a. For any postings to the District's social network sites, employees must adhere to any and all posted disclaimers, privacy policies, terms of service, and terms of use.

b. Personal use of social networks will be limited to the employee's break and lunch times. Employees are not to use District email addresses to register on social networks, blogs, or other

online tools utilized for personal use.

c. Only employees authorized by the District will be allowed to identify themselves as representatives of the District. Employees are not otherwise authorized to comment for the District and should direct any media/public inquiries to the District's Public Information Officer. Employees authorized to do so will bear the responsibility for representing the District in a professional manner.

d. Dissemination of information that could be considered confidential, proprietary, or somehow sensitive in nature is not to be discussed or referred to on such sites. Any request for this type of information needs to adhere to the regular and normal channels of public information requests.

e. Use of any social networking or media is not to interfere with employee's primary job responsibilities.

f. Employees should express only their personal opinions if they have not been authorized by the District to act as a District representative on social media. If the District is a subject of the content the employee is creating, the employee must be clear and open about the fact that the individual is an employee and make it clear that the employee's views do not necessarily represent those of the District, fellow employees, customers, suppliers, or people working on behalf of the District. If an employee does publish a blog or post online related to the employee's work they do or subjects associated with the District, the employee must make it clear that the employee is not speaking on behalf of the District. It is best to include a disclaimer such as, "*The postings on this site are my own and do not necessarily reflect the views of Carmichael Water District*."

g. The District prohibits taking negative action against any employee for reporting a possible deviation from this policy or for cooperating in an investigation. Any employee who retaliates against another employee for reporting a possible deviation from this policy or for cooperating in an investigation is a violation of this policy.

h. Employee conduct – both inside and outside of the workplace – that adversely affects the employee's job performance, the performance of fellow employees, or otherwise adversely affects customers, suppliers, people who work on behalf of the District, or the District's legitimate business interests may result in a violation of this policy.

i. Nothing in the District's Social Media Policy is designed to interfere with, restrain, or prevent employee communications regarding wages, hours, or other terms and conditions of employment.

3040.110 Disciplinary Action

Any violation of this policy may result in disciplinary action depending on the severity of the violation. Disciplinary action may include verbal warning though immediate termination.