POLICY 61.030 – DEPARTMENT COMMUNICATION SYSTEMS/EQUIPMENT

Date:	July 2023
Revision No:	4
Supersedes:	July 2022
First Adopted:	April 24, 2018

POLICY:

The Department provides employees with communication systems and/or equipment necessary, and to an extent practicable, to promote the efficient conduct of business. Examples of Department provided communication systems and equipment include, but are not limited to all telephone, radio, computer, mobile data computers, voicemail, fax machines/systems, pagers, email, internet access, wireless access, cell phones, smart phones, tablets, and all other computer and/or computer related communication systems. All such communication systems and equipment are to be used as prescribed within this policy.

The purpose of this policy is to ensure the responsible and acceptable use of all of the Department's communication systems and/or equipment resources noted above, as well as those technologies which may be introduced in the future. This policy applies to all employees who utilize this equipment or are provided access to these systems.

PROCEDURE:

Communications Systems and/or Equipment Privacy:

The Department's communications systems and/or equipment and all information stored on them, or on removable media, are provided at the Department's expense and are the Department's sole property. Communications are not private; they are business records that can be reviewed by the Department or subpoenaed under law and may be accessible to the public pursuant to the Freedom of Information Act (FOIA) and California Public Records Act (CPRA). Accordingly, employees should have no expectation of privacy regarding any communication, business related or personal, that they create, send, receive, or store on any of the Department's communication

systems, equipment, or removable media.

The Department reserves the right to access, monitor, and review the use of its communication systems, as well as to retrieve the data that is stored and transmitted, for training purposes, quality assurance purposes, and to determine if there have been any breaches of security or confidentiality, misuse, or other violations of Department policy. The Department may inspect the contents of any device at any time, for any reason, including purposes of investigation.

Communication Systems and/or Equipment Security:

A. San Bernardino Municipal Water Department (SBMWD) discourages and does not require employees to use personal equipment for business operations. Those employees who may use their personal devices for log in through Microsoft 365 must abide by the policy herein as applicable. Written approval from Information Technology and the Division Director must be obtained prior to using any personal devices including portable computers, portable storage media, mobile devices or software for any other business operations. SBMWD is not responsible for the purchase or costs associated with the use of personal devices. SBMWD Personally Identifiable Information or Sensitive Information must not be stored on personal devices. At no time does the Department accept liability for the security of the personal device when accessing Department networks. Information Technology may, without notification, prevent or ban any personal device which disrupts any Department computing resource or is used in a manner which violates any Department policy. Additional key mandatory policies include but are not limited to Policy #62.060 Use of Personal Cell Phones, and Policy #62.070 Social Media.

B. Employees shall not share passwords with others unless authorized to do so (refer to Policy No. 61.040 – Passwords). The Department retains the right to access Department provided communication systems even when protected by passwords or codes. Employees should not construe the use of passwords or codes as creating an expectation of privacy.

C. Regardless of whether the Department has chosen to monitor any or all of the communication systems and/or equipment, either in the past or at any time in the future, the Department’s right to monitor such systems and/or equipment is not, and may not, be waived. Employees should not consider the Department’s choice not to monitor as creating an expectation of privacy. All employees shall understand and agree that there is no expectation of privacy for any

communication sent or received by Department owned communication systems and/or equipment. Any personal computing device used for business purposes is also subject to search and review as a result of litigation that involves the Department.

- No employee should expect a guarantee of privacy in communications over the Internet and SBMWD network.
- Violations of this Policy may be discovered by routine maintenance and active monitoring of SBMWD electronic communication systems and network, any method stated in this Policy, or pursuant to any legal means.

D. To ensure that software is properly installed according to manufacturer's specification and in order to avoid system malfunctions and/or failure, the Information Technology section will coordinate the purchase and installation of all software.

D. Employee or consultant owned software or removable media may not be installed on Department owned or personal computers without the prior authorization of the Information Technology section. If approved, only original installation media or assigned software keys may be used. The Information Technology section will archive and inventory the installation media, software keys, and license agreements.

E. Computer systems are at risk of being invaded by viruses or other malware through loaded software or downloaded material through the Internet or other sources. Only software acquired through licensing agreements or shared software through public domain that is authorized by the Information Technology section under the direction of the Deputy General Manager may be loaded onto Department computers or any personal device. All foreign removable media are prohibited from use without prior authorization by the Information Technology section under the direction of the Deputy General Manager. External attachments or website links (URLs) shall not be opened if the attachment or links are suspicious, from an unknown source, sent with executable file extensions, (e.g., ".exe", "vbs", "msi") files, or are otherwise unexpected by the recipient. All programs, files, or macros downloaded from the Internet shall be scanned immediately for computer viruses. If a virus is detected, the Information Technology section must be notified immediately.

F. Employees shall not attempt to provide any computer system, files, or messages to others without proper authorization or gain unauthorized access to remote computer systems. Further, employees shall not damage, alter, or disrupt any computers

or systems in any way. Employees shall not use another's code or password or disclose anyone's code or password, including their own. Employees shall not enable unauthorized third parties to have access to or use the Department's communication systems and/or equipment. The Information Technology section will approve and/or arrange access for any third party that legitimately requires such access, as appropriate. In addition, employees shall not otherwise jeopardize the security of the Department's communication systems and/or equipment.

G. All electronic data files must be stored on the Department file server and not on the local hard drive, unless approved by the Information Technology section under the direction of the Deputy General Manager. If a laptop is being used, electronic data should be copied to the file server at least once a week.

H. All employees have an affirmative duty to report any abuse or misuse of any Department systems and/or equipment to their Division Director or the Information Technology section immediately. Failure to do so may result in disciplinary action up to and including termination.

Communication Systems and/or Equipment Acceptable Use:

A. The Department's communication systems are to be used to conduct Department business. Personal use of any Department system (such as a telephone call or email to/from family and friends, etc.) should be avoided whenever possible and kept to a minimum. Although the Department recognizes that certain limited de minimus personal use of Department systems and/or equipment may occur, all employees understand and agree that all messages and information created, generated, and/or received on Department systems or equipment shall be treated the same as business related communications. Thus, all employees should be aware that all personal communications made using Department communication systems or equipment are subject to monitoring. Employees have no expectation of privacy in any such personal communication, or any other communication made with and/or received by Department communication systems or equipment.

B. All employees should be aware that any expense(s) caused by personal and/or unauthorized use of Department systems and/or equipment shall be the sole responsibility of the employee who caused the expense(s) to be incurred. Such expenses shall include, but are not limited to, long distance or toll charges, Internet charges, service charges, international data charges, purchases over the Internet, etc. Any employee incurring such expenses shall reimburse the Department for

the entire amount of such costs and expenses, as well as any additional return or cancellation fees that may be incurred.

C. Utilization of the Internet shall be for Department business. Occasional de minimus use of the Internet for personal use is allowed. Internet usage is filtered and logged by the Department and may be used for determining individual compliance with this policy.

Employees should exercise care in accessing or copying any information which does not belong to the Department. Almost all data and software are subject to Federal copyright laws. Software which requires purchase or reimbursement for its use, such as "Shareware", requires strict adherence to the terms and conditions of the owner unless written permission for unrestricted use has been obtained. When in doubt, each employee is tasked with consulting Information Technology staff. All downloaded files become the property of the Department, must be properly licensed and registered and must have a direct business use.

D. The Department reserves its right to monitor de minimus personal use of all communication systems and/or equipment. De minimus use has been defined to include periodic communications with family and friends, Department approved educational sites, and periodic miscellaneous personal correspondence via any of the Department's systems and/or equipment. The Department prohibits the use of the internet, or any other communication technology subsidized by the Department to stream audio or video content not related to official department business, from either a Department or personal device.

E. When using the Department's communication systems and/or equipment, employees shall use the same standards of care and professionalism as used in other business communications. Individual users must be aware of, and at all times attempt to prevent, potential Department liability in their use of its communications systems and/or equipment.

F. All usage shall be in full compliance with all copyrights and licensing agreements.

G. Employees shall not represent the Department on social media without authorization, refer to Policy No. 62.070 Social Media.

H. Examples of prohibited use of Department communication systems and/or equipment include, but are not limited to:

a. Sending abusive, threatening, or harassing messages,

including those containing racial epithets, ethnic slurs, or any other language involving the harassment of others.

b. Faxing, downloading, transmitting, distributing, or possessing sexually explicit, harassing, or otherwise objectionable materials.

c. Use of communication systems for chain letters, inappropriate or objectionable jokes, pools or other sorts of gambling, non-professional chat rooms, online game rooms, illegal activities, listservs, or news groups for non-Department purposes.

d. Engaging in solicitation or proselytizing for non-Department related commercial, religious, political, or other causes.

e. Furthering an employee's secondary employment outside the employee's scope of employment with the Department. Employees may not create content or perform tasks for self-owned or any other business entities on the Internet, using Department-owned equipment or Department access.

f. Passing off personal views as representing those of the Department.

g. Electronic forgery.

h. Unauthorized encryption tools and/or technology.

i. Engaging in any improper activity that could adversely affect the Department.

The communication of proprietary or confidential information via any Department system or equipment without prior approval by the Information Technology section.

I. An employee who receives harassing/offensive or inappropriate messages should immediately report the incident in accordance with the Department's harassment policy.

J. An employee who receives an email message he/she finds offensive shall immediately report receipt of the message to their supervisor, Director, the Information Technology Manager, or the Deputy General Manager. An employee who inadvertently accesses an Internet site that is prohibited under the Department's security rules shall immediately report the incident the Information Technology Manager or

supervisor. Failure of an employee to report incidents covered by this paragraph shall be deemed to constitute voluntary participation in the inappropriate communication or unintentional attempted access to prohibited Internet material and may be subject to discipline up to and including termination.

K. Employees must return their communication equipment to the Department when no longer required for their work assignment and/or upon separation from the Department. Department issued communication equipment, including cell phone and telephone number, is the property of the Department. Persons separated from Department employment may not take the equipment or telephone number with them unless approved by the General Manager. If the General Manager determines that the fair market value of the cell phone is minimal, he/she may authorize the individual to pay the fair market value to the Department and keep the equipment.

L. Reasonable care should be taken to prevent equipment loss or damage. Employees who have Department issued equipment for take home purposes and/or are traveling with Department communication equipment, are expected to keep the communication equipment secure. Communication equipment should be kept within reach. When it is necessary to leave equipment, it should be stored in a locked environment and out of sight. Employees are responsible for the cost of intentional damage or reckless loss of assigned communication equipment.

Due to limited resources, the Department is not able to offer all of the available communication technologies to every employee. However, all employees who use the available communication technologies are responsible for learning, via in-house or outside training opportunities; the various technologies offered them in order to perform their duties effectively. Any access to the communication systems and/or equipment provided by the Department is a privilege and is revocable at any time for any reason.

Policy Review

Board Approved:	5/8/2018
No Changes:	7/2019
Revision Board Approved:	5/12/2020
Minor changes GM Approved:	7/2021
Minor changes GM Approved:	7/2022
Revision Board Approved:	8/22/2023
Spacing/grammar/font changes:	7/2024

ACKNOWLEDGEMENT OF MANDATORY COMPLIANCE WITH CITY OF SAN BERNARDINO MUNICIPAL WATER DEPARTMENT POLICY ON DEPARTMENT COMMUNICATION SYSTEMS/EQUIPMENT

I hereby acknowledge receipt of the City of San Bernardino Municipal Water Department Policy on Department Communication Systems/Equipment (Policy No. 61.030). I have read the policy and understand that compliance with this policy is mandatory, and violation of this policy may result in discipline up to and including termination.

_____ _____

Date Employee Signature

_____

Employee Name (Print)