

**MEETING OF THE ADMINISTRATIVE COMMITTEE
OF THE BOARD OF DIRECTORS
WATER REPLENISHMENT DISTRICT OF SOUTHERN CALIFORNIA
4040 PARAMOUNT BOULEVARD, LAKEWOOD, CALIFORNIA 90712
12:00 P.M., MONDAY, FEBRUARY 14, 2011**

AGENDA

Each item on the agenda, no matter how described, shall be deemed to include any appropriate motion, whether to adopt a minute motion, resolution, payment of any bill, approval of any matter or action, or any other action. Items listed as "For information" or "For discussion" may also be the subject of an "action" taken by the Board or a Committee at the same meeting.

- 1. DETERMINATION OF QUORUM**
- 2. PUBLIC COMMENT**
- 3. MINUTES OF THE MEETING OF JANUARY 10, 2011**
Staff Recommendation: Approve as submitted.
- 4. CALIFORNIA ENVIRONMENTAL QUALITY ACT (CEQA) POLICY**
Staff Recommendation: For discussion.
- 5. PROPOSED ADMINISTRATIVE CODE AMENDMENTS TO CHAPTER 12 -
ELECTRONIC MEDIA/INTERNET POLICY**
Staff Recommendation: For discussion.
- 6. SALARY INFORMATION**
Staff Recommendation: For discussion.
- 7. DEPARTMENT REPORT**
- 8. DIRECTOR'S REPORTS, INQUIRIES AND FOLLOW-UP OF DIRECTIONS TO
STAFF**
- 9. ADJOURNMENT**

Posted by Abigail C. Andom, Deputy Secretary, February 10, 2011.

In compliance with the Americans with Disabilities Act (ADA), if special assistance is needed to participate in the Board meeting, please contact Deputy Secretary Abigail Andom at (562) 921-5521 for assistance to enable the District to make reasonable accommodations.

All public records relating to an agenda item on this agenda are available for public inspection at the time the record is distributed to all, or a majority of all, members of the Board. Such records shall be available at the District office located at 4040 Paramount Boulevard, Lakewood, California 90712.

Agendas and minutes are available at the District's website, www.wrd.org.

In compliance with the Americans with Disabilities Act (ADA), if special assistance is needed to participate in the Board meeting, please contact Deputy Secretary Abigail Andom at (562) 921-5521 for assistance to enable the District to make reasonable accommodations.

All public records relating to an agenda item on this agenda are available for public inspection at the time the record is distributed to all, or a majority of all, members of the Board. Such records shall be available at the District office located at 4040 Paramount Boulevard, Lakewood, California 90712.

Agendas and minutes are available at the District's website, www.wrd.org.

UNAPPROVED
MINUTES

UNAPPROVED
MINUTES

**MINUTES OF JANUARY 10, 2011
MEETING OF THE ADMINISTRATIVE COMMITTEE
OF THE BOARD OF DIRECTORS
WATER REPLENISHMENT DISTRICT OF SOUTHERN CALIFORNIA**

A meeting of the Administrative Committee of the Board of Directors of the Water Replenishment District of Southern California was held on January 10, 2011 at 12:35 p.m. at the District Office, 4040 Paramount Boulevard, Lakewood, California. Chairperson Willard H. Murray, Jr. called the meeting to order and presided thereover. Deputy Secretary Abigail C. Andom recorded the minutes.

1. DETERMINATION OF QUORUM

Attendees included:

Committee: Directors Willard H. Murray, Jr. and
Lillian Kawasaki

Staff: Scott Ota, Interim District Counsel Francisco Leal

2. PUBLIC COMMENT

None.

**3. MINUTES OF THE MEETINGS OF NOVEMBER 8, 2010 AND
DECEMBER 13, 2010**

The minutes of November 8, 2010 were approved as submitted.
The minutes of December 13, 2010 were received and filed.

4. CALIFORNIA ENVIRONMENTAL QUALITY ACT (CEQA) POLICY

Chief Financial Officer Scott Ota stated that the item will be handled by Special Counsel Ed Casey who will provide an update at next month's meeting.

**5. PROPOSED ADMINISTRATIVE CODE AMENDMENTS –
CHAPTER 12 ELECTRONIC MEDIA/INTERNET POLICY**

Interim District Counsel Francisco Leal stated that former counsel proposed amendments to the District's electronic media and internet policy which they will review for provide an update at next month's meeting.

6. SALARY INFORMATION

Mr. Ota stated that staff received a request from the State Controller's office regarding salary information of District employees and Board members. He stated that the deadline to submit the information requested was January 14, 2011.

Discussion followed. The Committee requested Mr. Ota to send the Board members the information provided to the State

Controller's office. The Committee also requested further discussion of discretionary posting of the salary information at the District's web site at next month's meeting.

7. WORK SCHEDULE

Director Murray stated that he would like to recommend changing the work schedule of non-union employees of the District to work at minimum a five-day, forty-hour per week schedule and continue to offer the flexible 9-80 work schedule for union exempt and non-exempt employee members of the District's collective bargaining unit.

Director Kawasaki stated that she cannot support Director Murray's recommendation and would like to keep the 9-80 work schedule for all District employees.

The Committee requested the item be agendaized for the January 21, 2011 Board meeting with a split vote from the Committee.

8. DEPARTMENT REPORT

Mr. Ota provided an update on the Department's activities.

9. DIRECTOR'S REPORTS, INQUIRIES AND FOLLOW-UP OF DIRECTIONS TO STAFF

Director Kawasaki requested an update of pending items be discussed at next month's meeting.

10. ADJOURNMENT

With no other business to come before the Committee, the meeting was adjourned at 1:50 p.m.

Chair

ATTEST:

Member



MEMORANDUM

ITEM NO. 4

Prepared by: J H Shaunessy

Reviewed by: Scott M Ota

Approved by: Robb Whitaker

DATE: FEBRUARY 14, 2011

TO: ADMINISTRATIVE COMMITTEE

FROM: ROBB WHITAKER, GENERAL MANAGER

SUBJECT: CALIFORNIA ENVIRONMENTAL QUALITY ACT (CEQA) POLICY

SUMMARY

Director Kawasaki has requested that Special Counsel be present to discuss the possibility of a CEQA policy for applicable District projects.

FISCAL IMPACT

None.

STAFF RECOMMENDATION

For discussion.



MEMORANDUM

ITEM NO. 5

Prepared by: Scott Ota

Reviewed by: J H Shaunessy

Approved by: Robb Whitaker

DATE: FEBRUARY 14, 2011

TO: ADMINISTRATIVE COMMITTEE

FROM: ROBB WHITAKER, GENERAL MANAGER

SUBJECT: PROPOSED ADMINISTRATIVE CODE AMENDMENTS TO CHAPTER 12 -
ELECTRONIC MEDIA/INTERNET POLICY

SUMMARY

For your consideration and direction, attached is amended Chapter 12 of the Administrative Code, which includes a proposed Email Retention Policy ("Policy").

The Policy applies to emails of District officials, offices, employees, volunteers and contractors. The Policy also clearly identifies the types of emails that constitute public records and those that do not. For instance, the following definition of "public records" has been incorporated in the Policy: "any writing or recording of an event or information, which is kept in the custody of a public officer, either because a law requires it to be kept or because it is necessary or convenient to the discharge of the public officer's duties, and was made or retained for the purpose of preserving its information content for future reference".

Permanent District electronic records are subject to disclosure in accordance with the California Public Records Act ("CPRA"). Generally, emails that contain substantive information concerning the District's policies, decision-making, proceedings, projects, or contractors, or that may later be important or useful for carrying out the District's business should be retained as public records in accordance with the Policy and subject to the District's Records Retention Policy and Schedule.

Pursuant to the Policy, regardless of the retention requirements, emails and other electronic or paper documents pertaining to threatened or actual legal proceedings must be retained until the litigation is finally concluded.

The Policy further provides that because emails and email systems may not be used for permanent storage of District records, the emails are generally deemed to constitute preliminary drafts, notes, or interagency or intra-agency memoranda that are not retained by the District in the ordinary course of business and that are therefore exempt from disclosure pursuant to the CPRA. Pursuant to the Policy, the District's General Manager and Assistant General Manager are responsible for determinations concerning disclosure of District records, including emails, in response to requests pursuant to CPRA, subpoena or court order and as authorized by the District's Administrative Code. When a request for disclosure of District records that applies to emails is received, the person responsible for the covered records must, using his/her best efforts and by any lawful means available, preserve any email covered by the request until it is determined whether the email is subject to retention and/or disclosure. The General Manager, Assistant General Manager, and/or District Counsel must be contacted

concerning any request for disclosure of District records that applies to email in the possession of District officials, officers and employees.

Finally, the Policy also provides that back-up tapes are only for disaster recovery purpose and that back-up copies performed by Information Technology staff are not records retention. We suggest that back-up tapes should be retained for no more than six (6) months. This time frame may, however, be increased or decreased, at Administrative Committee's direction and recommendation.

FISCAL IMPACT

None.

STAFF RECOMMENDATION

For discussion.

12 ELECTRONIC MEDIA/INTERNET POLICY

This Chapter shall be known as the District's Electronic Media and Internet Policy ("Policy"). The District provides various electronic facilities and technology resources to authorized employees to assist them in the performance performing of their job duties for the District. Each employee has a responsibility to use these District resources in a manner that increases productivity, enhances the District's public image, and is respectful of other employees. Failure to follow the District's policies regarding the use of these resources may lead to disciplinary measures, up to and including termination of employment.

12.1 Policies Regarding Ownership of Information Stored on Electronic Media

All information, in any format, stored by any means on the District's electronic facilities (Voicemail, Electronic Mail, computer network drives, hard disks or individual diskettes) is the property of the District and subject to inspection whenever the District has reasonable suspicion that an employee has violated this policy or ~~for for any~~ legitimate business needs. Under those circumstances, the Board President, General Manager and ~~Assistant General Manager~~ Chief Financial Officer ~~Assistant General Manager~~ Chief Engineer shall have the ability, and reserve the right, to review any electronic media with or without consent. However, no other person has the right to go into any electronic media of another person for any purpose other than legitimate District business.

In addition to reviews of stored material by authorized District employees, users of District resources shall be aware that such material might be retrieved by unauthorized "hackers" who have only curiosity or mischief as a motive. Any District eEmployee caught abusing the District's electronic media will be held responsible for damages and will be disciplined, and may be up to and including terminated termination.

12.2 Safety and Integrity of Information Imported from Electronic Media

~~Information received from any source outside the District stored on removable media (such as diskettes or ZIP disks) must be virus-scanned before any files are opened or copied to the District network. Any authorized user of the District resources shall rRequest assistance from Information Systems if he or she does not you do not know how to do this.~~

12.312.2 Policies Regarding Electronic Mail

The official policy of the District is that all electronic mail ("E-mail") messages are treated as District correspondence. E-mail can be accessed by anyone on the network who has your password. Even the use of system passwords does not ensure confidentiality. Passwords

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Indent: Left: 0.74"

are designed for District security, not individual privacy. E-mail should not be used for non-District business. E-mail messages are not private. E-Mail should never be used to transmit confidential financial or personal ~~area~~ information.

a) Any communication by Ee-mail should be drafted with the same care as a formal memorandum. E-mail messages should not contain informal remarks that might potentially be embarrassing to the District, its employees, or its constituents. Never write anything you do not want forwarded. Your message could end up being read by someone you were not expecting to read it.

b) E-mail messages must never contain offensive, abusive or harassing language. This includes, but is not limited to, the display or transmission of sexually explicit images, cartoons, jokes and messages or any other message that could bring discredit to the District. Employees should also refrain from using information in a way that would be disruptive, offensive, or harmful to morale. For example, the creation, display, or transmission of sexually-explicit images, messages or cartoons, any use of ethnic slurs, racial epithets, or any conduct which violates the District's policy prohibiting discriminatory conduct or harassment is strictly prohibited.

c) The District encourages employees to report if someone is sending you offensive, harassing or sexually explicit e-mail messages — whether it is internal or external e-mail — to the General Manager ~~or the Assistant General Manager / Chief Engineer, or the Manager of Administration~~ Chief Financial Officer ~~Assistant General Manager~~. The District has a policy regarding discrimination or harassment of its employees and will not tolerate these actions. There will be no retaliation against an employee who makes any good faith complaint.

d) E-mail should never be used to solicit for charities, schools or personal business.

— An eE-mail instruction or request from a constituent, outside contractor, or other business contact is no less important than one in a letter. Therefore, employees should not erase their external eE-mail messages (either incoming or outgoing) until doing the following: Employees should print hard copies of these external (incoming and outgoing) e-mail messages and send them to the appropriate file or other permanent file. Once the copy has been made and forwarded to the file, the e-mail message should be deleted from the system.

Formatted: Text 1.1a Code, Indent: Left: 0.74", Numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0.81" + Tab after: 0.46" + Indent at: 1.01"

Formatted: Bullets and Numbering

Formatted: Indent: Left: 0.81"

12.3 Electronic Mail Retention Policy

This section governs retention of e-mail, or electronic communication, that is created, sent, received, forwarded, edited, stored, or otherwise used by means of District electronic information resources of any kind, including, but not limited to, computers, computer networks, software, telephones, voicemail, personal data assistants, and any other electronic data systems or equipment. This policy applies to eE-mails of District officials, officers, employees, volunteers and contractors (collectively referred to as "Authorized Users").

Emails may consist of correspondence and other documentation which may constitute District records subject to the requirements of the California Public Records Act ("CPRA"), the District's Records Retention Schedule and the laws and regulations governing it, and other laws and regulations that apply to public agency information.

E-mail and E-mail systems are intended to be a medium of communication. E-mail and E-mail systems are not intended to be and may not be used for the electronic storage or maintenance of permanent District records. Back-up tapes are for disaster recovery purposes only. Retention is the responsibility of the sender of the message, not the back-up process. Back-up copies performed by Information Technology staff are *not* records retention. Back-up tapes should be retained no more than — ~~(suggested retention period: 6 months)~~ 3 years 6 months.

Authorized users are responsible for determining whether E-mails created, received, or used by them should be retained as permanent District public records. The definition of **public records** is "any writing or recording of an event or information, which is kept in the custody of public officer, either because a law requires it to be kept or because it is necessary or convenient to the discharge of the public officer's duties, and was made or retained for the purpose of preserving its information content for future reference." Typically, E-mails that contain substantive information concerning District policies, decision-making, proceedings, projects, or contractors, or that may later be important or useful for carrying out District business should be retained as permanent District records in accordance with this policy and District's Records Retention Schedule. Such E-Mails must be stored at ~~[Instructions pertaining to storage of permanent electronic records should be inserted here]~~ and deleted. All other

E-mails that should be retained as either permanent or non-permanent records pursuant to the Records Retention Policy, should

Formatted: Font: (Default) Arial

Formatted: Indent: Left: 0.81", First line: 0"

Formatted: Font: (Default) Arial

Comment [m1]: District's IT department should confirm whether the 6 months retention schedule would be acceptable, given District's systems.

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Indent: Left: 0.81", First line: 0"

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Bold

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

be printed, and filed or saved in the corresponding District file and deleted. The General Manager or Chief Financial OfficerAssistant General Manager and District Counsel are available to assist persons subject to this policy in determining which E-mails should be retained as permanent WRD records and how, and to address other questions concerning the application of this policy.

- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial

Regardless of retention requirements, E-mail and other electronic or paper documents pertaining to threatened or actual legal proceedings must be retained until the litigation is finally concluded. Examples of eE-mails that are not public records include Ee-mails from friends or family, and Ee-mails from one coworker to another inviting him or her to lunch or coffee.

- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial, Bold

Authorized Users should generally determine whether E-mails created, received or used by them should be retained as permanent City District records within ten (10) working days of creation, receipt or use of the District E-mail. Because E-mails and e-mail systems may not be used for permanent storage of District records, E-mails are generally deemed pursuant to this policy to constitute preliminary drafts, notes, or interagency or intra-agency memoranda that are not retained by the District in the ordinary course of business and that are therefore exempt from disclosure pursuant to the CPRA. However, the District's General Manager and Chief Financial OfficerAssistant General Manager are responsible for determinations concerning disclosure of District records, including E-mails, in response to requests pursuant to the CPRA, subpoena or court order.

- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial

Comment [m2]: This time frame may be increased or decreased, at the direction of the Administrative Committee and approval by the Board of Directors.

- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial

Upon request for disclosure of District records that applies to E-mails, Authorized Users responsible for the covered records must, using his/her best efforts and by any lawful means available, preserve any E-mail covered by the request until it is determined whether the E-mail is subject to retention and/or disclosure. The General Manager, Chief Financial OfficerAssistant General Manager, and/or District Counsel must be contacted concerning any request for disclosure of District records that applies to E-mail in the possession of District officials, officers, employees and volunteers.

- Formatted: Font: (Default) Arial
- Formatted: Indent: Left: 0.81"

- Formatted: Font: (Default) Arial

Authorized Users are responsible for managing E-mail and E-mail systems used by them in accordance with this policy. Authorized Users should regularly review their mailboxes or folders that contain E-mails and delete E-mails that are not required to be kept by law or pursuant to this policy, or that are unnecessary or inconvenient for the discharge of official District duties or the conduct of District business, or that are otherwise no longer needed in accordance with this policy.

- Formatted: Indent: First line: 0"
- Formatted: Indent: Left: 0.81", First line: 0"
- Formatted: Font: (Default) Arial
- Formatted: Font: (Default) Arial

12.4 Policies Regarding Internet Usage

Use of the Internet is limited to business purposes only. Accessing information for personal use and/or with no business relevance, including sites that are inconsistent with the District's ethics and values, could discredit the District, or could lead to embarrassment and possibly legal consequences to the employee and the District, is prohibited. Non-business use also consumes resources, such as employee time and Internet connection bandwidth that could otherwise be used for the benefit of the District.

Where the District has a reasonable suspicion that this policy is being violated by an employee or has legitimate business need, the General Manager and the Assistant General Manager / Chief Engineer, Chief Financial Officer, Assistant General Manager reserve the right to record and monitor employee activity on the Internet when such activity takes place using the District's resources, login ID, and/or from District premises. Any Employee discovered abusing the District's Internet resources and policy will be held responsible for damages and will be disciplined, up to and including termination.

12.5 Access to Internet

Each person is responsible and accountable for his or her use of Internet resources. Access will be provided to District employees whom the District determines have a legitimate business need for it.

12.6 Individual Accountability

Many people use the Internet under the illusion that their actions are private and anonymous. This is not so. Every time you visit a site, you leave a calling card that reveals where you come from, what kind of computer you have, and other details about your identity and viewing habits. Most sites keep logs of all your visits. Remember: All access to the Internet from within the District network, or using the District login ID, is tagged with the District's name. This will appear in e-mail addresses, interactive sessions, and in other systems' operational logs — just as if a business card bearing the District logo was being provided when accessing the Internet. Individuals should conduct work on the Internet in accordance with established District ethics, values and business practices as described below, and elsewhere in this Administrative Code.

12.7 Internet Guidelines

All policies apply to Internet and related services including WWW, FTP, USENET groups, bulletin boards, Internet e-mail etc. Internet use must be consistent with District policies and provide business benefit.

- a) ~~The creation and/or usage of e-mail IDs for use while logged on to the Internet with the District login ID is prohibited.~~
- b) ~~The creation and/or receipt of e-mail messages from within any Internet Service Provider (ISP) are prohibited. External e-mail is to be sent from, and external e-mail received, through the District's e-mail system only.~~
- e) ~~_____~~ The downloading and usage of software obtained from the Internet is prohibited unless it is necessary to the performance of District duties and has been approved by the Network Administrator. Such software could compromise the District's entire computer network.
- d) ~~The downloading and usage of document files obtained from the Internet is permitted only if those files are virus-scanned by the user before opening. Request assistance from Information Systems if you do not know how to do this.~~
- e) ~~f) _____~~ Files with the filename extension ".exe" or ".zip" or any file(s) located on an FTP site may not be downloaded by any user except the ~~Assistant General Manager / Chief Engineer~~ Chief Financial Officer Assistant General Manager or the Network Administrator.
- f) ~~g) _____~~ Data and informational integrity should be considered questionable when obtained from the Internet. Care must be taken to ensure the validity of information before using it in District business.
- g) ~~h) _____~~ Consistent with other District policies and applicable law, the District reserves the right to monitor any Internet communication passing through District facilities.
- h) ~~i) _____~~ Employees, unless specifically authorized to do so by the General Manager or ~~Assistant General Manager / Chief Engineer~~ Chief Financial Officer Assistant General Manager, and only if such practices are validated under applicable law, are prohibited from entering into contractual agreements or making statements that may be interpreted as contractual via any Internet site.
- i) ~~j) _____~~ All Internet users should be aware of significant security problems that could negatively impact the District. Uncontrolled (i.e. no firewall protection) access allows infected or malicious code (viruses) to be sent to the District's computer network from the Internet and increases risk of unnoticed and unauthorized examination, export, modification, and/or destruction of proprietary information.

Formatted: Bullets and Numbering

1460977.1

Formatted: Font: 10 pt

12 ELECTRONIC MEDIA/INTERNET POLICY

This Chapter shall be known as the District's Electronic Media and Internet Policy ("Policy"). The District provides various electronic facilities and technology resources to authorized employees to assist them in the performance of their job duties for the District. Each employee has a responsibility to use these District resources in a manner that increases productivity, enhances the District's public image and is respectful of other employees. Failure to follow the District's policies regarding the use of these resources may lead to disciplinary measures, up to and including termination of employment.

12.1 Policies Regarding Ownership of Information Stored on Electronic Media

All information, in any format, stored by any means on the District's electronic facilities (Voicemail, Electronic Mail, computer network drives, hard disks or individual diskettes) is the property of the District and subject to inspection whenever the District has reasonable suspicion that an employee has violated this policy or for any legitimate business needs. Under those circumstances, the Board President, General Manager and Assistant General Manager shall have the ability, and reserve the right, to review any electronic media with or without consent. However, no other person has the right to go into any electronic media of another person for any purpose other than legitimate District business.

In addition to reviews of stored material by authorized District employees, users of District resources shall be aware that such material might be retrieved by unauthorized "hackers" who have only curiosity or mischief as a motive. Any District employee caught abusing the District's electronic media will be held responsible for damages and will be disciplined and may be terminated.

12.2 Policies Regarding Electronic Mail

The official policy of the District is that all electronic mail ("E-mail") messages are treated as District correspondence. E-mail can be accessed by anyone on the network who has your password. Even the use of system passwords does not ensure confidentiality. Passwords are designed for District security, not individual privacy. E-mail should not be used for non-District business. E-mail messages are not private. E-Mail should never be used to transmit confidential financial or personal information.

- a) Any communication by E-mail should be drafted with the same care as a formal memorandum. E-mail messages should not contain informal remarks that might potentially be embarrassing to the District, its employees or its constituents. Never write anything you

do not want forwarded. Your message could end up being read by someone you were not expecting to read it.

- b) E-mail messages must never contain offensive, abusive or harassing language. This includes, but is not limited to, the display or transmission of sexually explicit images, cartoons, jokes and messages or any other message that could bring discredit to the District. Employees should also refrain from using information in a way that would be disruptive, offensive or harmful to morale. For example, the creation, display or transmission of sexually-explicit images, messages or cartoons, any use of ethnic slurs, racial epithets or any conduct which violates the District's policy prohibiting discriminatory conduct or harassment is strictly prohibited.
- c) The District encourages employees to report if someone is sending you offensive, harassing or sexually explicit e-mail messages — whether it is internal or external e-mail — to the General Manager or the Assistant General Manager. The District has a policy regarding discrimination or harassment of its employees and will not tolerate these actions. There will be no retaliation against an employee who makes any good faith complaint.
- d) E-mail should never be used to solicit for charities, schools or personal business.

An E-mail instruction or request from a constituent, outside contractor, or other business contact is no less important than one in a letter. Therefore, employees should not erase their external E-mail messages (either incoming or outgoing) until doing the following: Employees should print hard copies of these external (incoming and outgoing) e-mail messages and send them to the appropriate file or other permanent file. Once the copy has been made and forwarded to the file, the e-mail message should be deleted from the system.

12.3 Electronic Mail Retention Policy

This section governs retention of e-mail, or electronic communication, that is created, sent, received, forwarded, edited, stored or otherwise used by means of District electronic information resources of any kind, including, but not limited to, computers, computer networks, software, telephones, voicemail, personal data assistants and any other electronic data systems or equipment. This policy applies to E-mails of District officials, officers, employees, volunteers and contractors (collectively referred to as "Authorized Users").

Emails may consist of correspondence and other documentation which may constitute District records subject to the requirements of the California Public Records Act ("CPRA"), the District's Records

Retention Schedule and the laws and regulations governing it, and other laws and regulations that apply to public agency information.

E-mail and E-mail systems are intended to be a medium of communication. E-mail and E-mail systems are not intended to be and may not be used for the electronic storage or maintenance of permanent District records. Back-up tapes are for disaster recovery purposes only. Retention is the responsibility of the sender of the message, not the back-up process. Back-up copies performed by Information Technology staff are *not* records retention. Back-up tapes should be retained no more than 6 months.

Authorized users are responsible for determining whether E-mails created, received, or used by them should be retained as permanent District public records. The definition of **public records** is "any writing or recording of an event or information, which is kept in the custody of public officer, either because a law requires it to be kept or because it is necessary or convenient to the discharge of the public officer's duties and was made or retained for the purpose of preserving its information content for future reference." Typically, E-mails that contain substantive information concerning District policies, decision-making, proceedings, projects, or contractors, or that may later be important or useful for carrying out District business should be retained as permanent District records in accordance with this policy and District's Records Retention Schedule.

E-mails that should be retained as either permanent or non-permanent records pursuant to the Records Retention Policy, should be **printed, filed or saved in the corresponding District file and deleted**. The General Manager or Assistant General Manager and District Counsel are available to assist persons subject to this policy in determining which E-mails should be retained as permanent WRD records and how to address other questions concerning the application of this policy.

Regardless of retention requirements, **E-mail and other electronic or paper documents pertaining to threatened or actual legal proceedings must be retained until the litigation is finally concluded**. Examples of E-mails that are *not* public records include E-mails from friends or family, and E-mails from one coworker to another inviting him or her to lunch or coffee.

E-mails and e-mail systems may not be used for permanent storage of District records. E-mails are generally deemed pursuant to this policy to constitute preliminary drafts, notes or interagency or intra-agency memoranda that are not retained by the District in the ordinary course

of business and that are therefore exempt from disclosure pursuant to the CPRA. However, the District's General Manager and Assistant General Manager are responsible for determinations concerning disclosure of District records, including E-mails, in response to requests pursuant to the CPRA, subpoena or court order.

Upon request for disclosure of District records that applies to E-mails, Authorized Users responsible for the covered records must, using his/her best efforts and by any lawful means available, preserve any E-mail covered by the request until it is determined whether the E-mail is subject to retention and/or disclosure. The General Manager, Assistant General Manager, and/or District Counsel must be contacted concerning any request for disclosure of District records that applies to E-mail in the possession of District officials, officers, employees and volunteers.

Authorized Users are responsible for managing E-mail and E-mail systems used by them in accordance with this policy. Authorized Users should regularly review their mailboxes or folders that contain E-mails and delete E-mails that are not required to be kept by law or pursuant to this policy or that are unnecessary or inconvenient for the discharge of official District duties or the conduct of District business, or that are otherwise no longer needed in accordance with this policy.

12.4 Policies Regarding Internet Usage

Use of the Internet is limited to business purposes only. Accessing information for personal use and/or with no business relevance, including sites that are inconsistent with the District's ethics and values, could discredit the District, or could lead to embarrassment and possibly legal consequences to the employee and the District, is prohibited. Non-business use also consumes resources, such as employee time and Internet connection bandwidth that could otherwise be used for the benefit of the District.

Where the District has a reasonable suspicion that this policy is being violated by an employee or has legitimate business need, the General Manager and the Assistant General Manager reserve the right to record and monitor employee activity on the Internet when such activity takes place using the District's resources, login ID or from District premises. Any Employee discovered abusing the District's Internet resources and policy will be held responsible for damages and will be disciplined, up to and including termination.

12.5 Access to Internet

Each person is responsible and accountable for his or her use of Internet resources. Access will be provided to District employees whom the District determines have a legitimate business need for it.

12.6 Individual Accountability

Many people use the Internet under the illusion that their actions are private and anonymous. This is not so. Every time you visit a site, you leave a calling card that reveals where you come from, what kind of computer you have, and other details about your identity and viewing habits. Most sites keep logs of all your visits. Remember: All access to the Internet from within the District network, or using the District login ID, is tagged with the District's name. This will appear in e-mail addresses, interactive sessions, and in other systems' operational logs — just as if a business card bearing the District logo was being provided when accessing the Internet. Individuals should conduct work on the Internet in accordance with established District ethics, values and business practices as described below, and elsewhere in this Administrative Code.

12.7 Internet Guidelines

All policies apply to Internet and related services including WWW, FTP, USENET groups, bulletin boards, Internet e-mail etc. Internet use must be consistent with District policies and provide business benefit.

- a) The downloading and usage of software obtained from the Internet is prohibited unless it is necessary to the performance of District duties and has been approved by the Network Administrator. Such software could compromise the District's entire computer network.
- b) Files with the filename extension ".exe" or ".zip" or any file(s) located on an FTP site may not be downloaded by any user except the Assistant General Manager or the Network Administrator.
- c) Data and informational integrity should be considered questionable when obtained from the Internet. Care must be taken to ensure the validity of information before using it in District business.
- d) Consistent with other District policies and applicable law, the District reserves the right to monitor any Internet communication passing through District facilities.
- e) Employees, unless specifically authorized to do so by the General Manager or Assistant General Manager, and only if such practices are validated under applicable law, are prohibited from entering into contractual agreements or making statements that may be interpreted as contractual via any Internet site.
- f) All Internet users should be aware of significant security problems that could negatively impact the District. Uncontrolled (i.e. no

firewall protection) access allows infected or malicious code (viruses) to be sent to the District's computer network from the Internet and increases risk of unnoticed and unauthorized examination, export, modification, and/or destruction of proprietary information.

1460977.1



MEMORANDUM

ITEM NO. 6

Prepared by: Scott Ota
Reviewed by: J H Shaunessy
Approved by: Robb Whitaker

DATE: FEBRUARY 14, 2011
TO: ADMINISTRATIVE COMMITTEE
FROM: ROBB WHITAKER, GENERAL MANAGER
SUBJECT: SALARY INFORMATION

SUMMARY

The Board of Directors asked the Administrative Committee to review the possibility of placing WRD salaries on the WRD's website.

At the September 23, 2010 meeting of the Administrative Committee, the Committee asked staff to find out if there is any pending legislation related to posting of salaries for either District staff or Board of Directors members. Staff reported to the Committee on October 21, 2010 that there was no pending litigation requiring the posting of salaries. The Committee also asked staff to look into local government agencies and report on which of the local agencies are posting their salaries on their websites.

At the November 8, 2010 meeting of the Administrative Committee, the Committee asked staff to find out if the State Controller has any legal recourse or binding power to require WRD to submit salary information for posting on the State Controller's website. District Counsel stated that pursuant to Government Code Sections 12463 and 53892, the Controller has the authority to require the District to submit salary information for posting on the Controller's website.

At the December 13, 2010 meeting of the Administrative Committee, the Committee reviewed the item again and recommended that no action was necessary at that time and staff will await the request from the State Controller's office.

Subsequent to that meeting, the WRD has received an official request from the State Controller's Office to provide the Division of Accounting and Reporting with the following information:

- Each and every job position within the district, including those filled by elected or appointed board members, full-time, part-time, temporary or seasonal employees, volunteers, and vacancies for which the special district issues a W-2
- The total 2009 salary, compensation, and benefits paid by the district for each and every job position, even in cases where the job position was occupied for only a portion of the year, or where two or more persons occupied the same job position during different times of the year

This item has been brought back at the behest of the committee to discuss if recent events impact whether this information should be listed on the District website or if the State Controller's site is sufficient.

FISCAL IMPACT

None.

STAFF RECOMMENDATION

For discussion.



MEMORANDUM

ITEM NO. 7

Prepared by: J H Shaunessy

Reviewed by: Scott Ota

Approved by: Robb Whitaker

DATE: FEBRUARY 14, 2011

TO: ADMINISTRATIVE COMMITTEE

FROM: ROBB WHITAKER, GENERAL MANAGER

SUBJECT: DEPARTMENT REPORT

SUMMARY

Staff has been working on the following projects:

- Work with Legal Counsel on a public records request in accordance with the California Public Records Request (CPRA) Act received from Orchard Dale Water District requesting information going back over 12 years to 1999.
- Work with Legal Counsel on a public records request in accordance with the California Public Records Request (CPRA) Act received from Anthony Kingsley.
- Work with Interim District Counsel on procedures relating to the District and transitioning any outstanding items from previous District Counsel
- Work with Legal Counsel regarding items related to the District's negotiation with the labor union
- Brought new staff person, Dr. Cathy Chang, on board filling the spot of Water Quality Program Manager left vacate by retiree Hoover Ng
- Work with Legal Counsel on financial data and historical records related to the lawsuit against WRD's replenishment assessment
- Researched and brought Administrative Code issue before committee regarding educational reimbursement
- Work with Legal Counsel on a public records request in accordance with the California Public Records Request (CPRA) Act received from Sedgwick, Detert, Moran & Arnold, LLP on behalf of Central Basin Municipal Water District (CBMWD)
- Attended and prepared minutes for Board of Directors on 1/21/11
- Attended and prepared minutes for Special Board of Directors meeting on 2/11/11
- Attended and prepared minutes for Finance Committee meeting on 12/25/11
- Attended and prepared minutes for Administrative Committee meeting on 1/10/11
- Attended and prepared minutes for Water Resources Committee meeting on 2/2/11
- Continued work on various personnel, human resource and legal issues

FISCAL IMPACT

None

STAFF RECOMMENDATION

For information.