




**COMMUNICATIONS TECHNICAL
POLICY/PROCEDURE**

Policy No. 3200	Date Issued: May 1, 1998
Section: 3000 – Technical	Date Revised: May 15, 2020
SUBJECT: USE OF INTERNET AND E-MAIL	
APPROVED: 	
Dennis Kidd, General Manager	

The purpose of this policy is to provide guidelines for Internet and e-mail use. The Authority will not incur risks or liabilities for personal use of the Internet or e-mail nor permit employees to create any obligations or liabilities for the Authority. At no time is any employee allowed to use these systems to perform any illegal act, nor will they be allowed to access materials determined to be in violation of community and/or professional standards. At no time may Internet or e-mail use violate Authority policies, procedures, rules, regulations and/or written directives.

1.0 Acceptable Uses of the Internet and E-Mail

- 1.1 Internet access and e-mail addresses are provided for business reasons only, with the intent to facilitate business, provide efficient and effective means of communications, and maintain and enhance the Authority's image.
- 1.2 Use of e-mail and the Internet shall not interfere with official duties.
- 1.3 Dispatch workstations have restricted Internet access and are not to be used to access personal e-mail accounts, download any files, or install any unauthorized computer software.
- 1.4 Personal Use
 - 1.4.1 Employees may make incidental personal use of the Internet if that use meets the following criteria:
 - does not involve resources designated for confidential systems
 - does not directly or indirectly interfere with the Authority's operation of electronic communications resources

- does not interfere with the employee's work assignment
- does not burden the Authority with any additional costs
- does not bring discredit to the Authority or cast significant doubt on the employee's reliability or trustworthiness or otherwise effect an employee's ability to work efficiently or harmoniously with others
- does not otherwise constitute an unauthorized use under this or other Authority policies

1.4.2 Incidental personal use does not include use by non-employees, even if they are members of an employee's immediate family or employees working under a sub-contract. If there are any questions as to whether or not an employee's use meets these criteria, the employee should contact his or her supervisor for clarification.

1.4.2.1 Wireless Access Points (APs) provide direct access to the Internet without interaction with the Authority's Local Area Network (LAN). Non-employees may obtain access to the Internet for incidental personal use only through these APs.

1.4.2.2 The Employee Association provides a computer in the break room for personal use by employees. This computer does not access the Authority's LAN and may be used more broadly but still must not be used in violation of any Authority policies.

2.0 Prohibited Internet and E-Mail Uses

- 2.1 Use of departmental computers, equipment and/or networks to receive, access, display, store, print, copy or distribute any obscene, indecent, lewd, lascivious, sexually explicit/suggestive materials, harassing or discriminatory material, whether text or graphic is strictly prohibited.
- 2.2 Use of departmental computers, equipment and/or networks to receive, access, display, store, print, copy or distribute any material that violates Policy No. 1100 (Equal Employment Opportunity) or Policy No. 1120 (Unlawful Harassment), whether text or graphic is strictly prohibited.
- 2.3 Creating, downloading, viewing, storing, copying, or transmitting materials related to gambling, illegal weapons, terrorist operations, or criminal activities, is strictly prohibited.
- 2.4 Gaining unauthorized access to other systems is strictly prohibited.
- 2.5 Use of departmental computers, equipment and/or networks to receive, access, display, store, print, copy or distribute any material which violates Authority

policies, procedures, rules, regulations, or written directives, whether text or graphic, is prohibited.

- 2.6 Incidental personal use of departmental computers, equipment and/or networks that causes delay or disruption of service to any Authority system or network is prohibited. Examples include, but are not limited to, streaming video or audio, file sharing programs, and down/uploading large file attachments.
- 2.7 Creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailing, regardless of the subject matter, is prohibited.
- 2.8 Acquiring, using, reproducing, transmitting, or distributing private information, classified or other non-public data, copyrighted material (beyond fair use), proprietary data or other intellectual property is prohibited.
- 2.9 Conducting any unauthorized fund-raising activity, endorsing any product or service, and/or participating in any lobbying activity or political campaign activity is prohibited.
- 2.10 Conducting or supporting outside employment or business activities is prohibited. Examples include, but are not limited to, sending or receiving messages related to a part-time real estate or other business venture and/or selling or trading merchandise as part of a business venture.
- 2.11 Using another person's access passwords, logon information, email account or other individual security accounts is strictly prohibited. Employees shall not share their password or account access unless directed to do so by a supervisor.

3.0 Expectations of Privacy

- 3.1 In accordance with Policy No. 7090 (Use and Expectation of Privacy), there should be no expectation of privacy assumed by anyone using departmental computers, email accounts, equipment and/or networks and the Authority assumes no responsibility for privacy or lack thereof when using same.
 - 3.1.1 Employees shall not use personal accounts to exchange email or other information that is related to the official business of the Authority.

4.0 Management Review of Internet and E-Mail Use

- 4.1 All email messages sent through department-issued email accounts, including attachments, are considered department records. The Authority reserves the right to access, audit, or disclose, for any lawful reason, any message transmitted over its email system or stored on any Authority servers. Employees are expected to produce e-mail records in compliance with the California Public Records Act, upon request. It is recommended that users retain email messages for at least 90 days but not more than 365 days.4.2 Internet activity will be inspected quarterly for appropriate use by Systems

Division personnel and reported to the Systems Supervisor. If inappropriate use is discovered, the Systems Supervisor will forward the report to the appropriate supervisor or manager for further action.

- 4.3 Other departmental computers, equipment and/or networks will be inspected quarterly as their intrinsic capabilities and limitations allow. If inappropriate use is discovered, the Systems Manager will forward the report to the appropriate supervisor or manager for further action.