

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE	Number 90.62	Issue 2	Page 1 of 7
	Effective Date December 7, 2012		

1. PURPOSE

- 1.1 This regulation defines acceptable uses of the City's information and communications technology resources.
- 1.2 This regulation also defines unacceptable actions and uses of City information and communications technology resources.
- 1.3 The standards set forth in this regulation are minimum standards for City Departments. Departments may develop rules and procedures regarding department-specific use of information and communications technology resources in order to implement this policy. Departments may also develop more restrictive rules for the particular department, when required to comply with local, state or federal laws or regulations.

2. SCOPE

- 2.1 This regulation applies to all information and communications technology resources owned or leased by the City, or that are provided as a service to the City, including future emerging technologies that may be implemented, and activities using any City-paid accounts, subscriptions or other technology services, such as Internet and World Wide Web access, voice mail, and Email, regardless of where the activities are conducted.
- 2.2 This regulation applies to all City employees, volunteers, and other City agents, collectively referred to as "Individuals," using some or all of the City's Information and Communications Technology Resources.
- 2.3 The City's information and communications technologies are provided for the benefit of City Departments in providing public services.

3. DEFINITIONS

- 3.1 "IT" – Information Technology

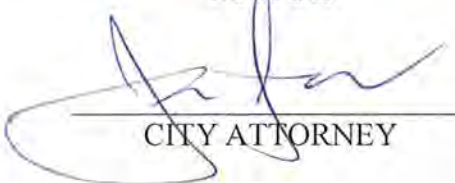
(Supersedes Administrative Regulation 90.62, Issue 1, effective October 1, 1996)

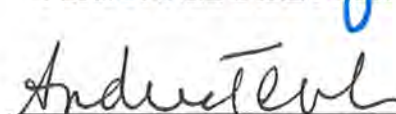
Authorized


MAYOR


PERSONNEL DIRECTOR


CITY CLERK


CITY ATTORNEY


INDEPENDENT BUDGET
ANALYST


CITY AUDITOR

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number 90.62	Issue 2	Page 2 of 7
INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE	Effective Date December 7, 2012		

- 3.2 “FTP” – File Transfer Protocol – A protocol used to transfer files between networked devices.
- 3.3 “Email” (Electronic Mail) – The electronic transfer of information typically in the form of electronic messages, memoranda, notes, meeting appointments, and attached documents from a sender to one or more recipients via a telecommunications network.
- 3.4 “Information and Communications Technology Resources” or “City IT Resources” – All technology resources owned or leased by the City and any City-paid accounts, subscriptions or other technology services. This includes office telephones, wireless/cellular telephones, smart phones, desktop and portable computer systems, printers fax machines, Internet and World Wide Web (Web) access, internal and external Email, electronic bulletin boards or newsgroups, file transfer protocol (FTP), other wireless systems, and emerging communications systems or devices.
- 3.5 “Internet” - is a network of networks connecting computer systems throughout the world. In addition to providing capability for Email, other Internet applications include, but are not limited to, news groups, FTP, telnet and the Web.
- 3.6 “Confidential” - For the purpose of this Administrative Regulation, confidential information refers to City information not authorized or intended to be disclosed outside the City. Such information shall only be accessible or disclosed to those individuals who have a business need to know, and shall not otherwise be disclosed unless disclosure is required by contract, ordered by a court, or required under applicable local, state, or federal laws or regulations. Confidential is not intended to cover City sensitive data category which is governed by state and federal law (e.g. social security numbers, credit card numbers, medical record information and etc.). Refer to AR90.64 for the Sensitive Data Administrative Regulation.

4. GENERAL POLICY

- 4.1 Use of City IT Resources shall be limited to work-related, City business purposes only. Personal files should not to be stored on City equipment.
- 4.2 When using the City's Email system, the Internet or other City IT Resources to communicate with others external to the City organization, individuals are representing the City of San Diego and therefore must communicate in a business-like manner. Refer to “Best Practices and Tips” on the CityNet site (located at Departments – Human Resources – Resources and Tools - Customer Service Best Practices and Tips) to ensure the communication is not in conflict with City policies or regulations.
- 4.3 The City's IT Resources and the data stored on them are the property of the City. An individual has no right of privacy in any information or data maintained in or on City IT

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number 90.62	Issue 2	Page 3 of 7
INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE	Effective Date December 7, 2012		

resources. Access to City IT Resources is a privilege which can be revoked at any time at the discretion of City management.

- 4.4 If during the course of employment, an individual performs or transmits work using City IT Resources, that work may be subject to the investigation, search, and review of others in accordance with this or other policies.
- 4.5 Unacceptable Uses: Notwithstanding any provisions of law to the contrary, the following uses of City IT Resources are expressly prohibited. This list does not necessarily include all possible unacceptable uses and may be expanded as new technologies emerge. The City retains the right to sanction individuals, as deemed appropriate, for unacceptable uses that may be defined later. Where a prohibited use is defined as “unauthorized” below, proper authorization must be requested in writing, in advance, through the Department of Information Technology or as otherwise directed.
- 4.5.1 Use of City telephones (landlines or wireless) for personal long distance calls. Such calls should be made through the use of a personal telephone credit card or with operator assistance and billed to the caller’s home telephone number.
- 4.5.2 Illegal activities including but not limited to fraud, theft, copyright infringement.
- 4.5.3 Use for personal profit, including the conducting of private commercial activities, solicitation or other personal business interest, or for the profit of another organization.
- 4.5.4 To conduct political activities as described by San Diego City Charter section 31 or San Diego Municipal Code section 27.3564(b).
- 4.5.5 To play online games or gamble.
- 4.5.6 To knowingly send, save, view or access material containing content that may be considered offensive to a reasonable person. Offensive material includes, but is not limited to, pornography, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes or images that would offend someone on the basis of his or her race, color, creed, sex, age, national origin or ancestry, physical or mental disability, veteran status, marital status, medical condition, sexual orientation, and any other category protected by federal, state, or local laws. Any use of City IT Resources to harass, threaten or discriminate is strictly prohibited by the City.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number	Issue	Page
INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE	90.62	2	4 of 7
	Effective Date December 7, 2012		

- 4.5.7 To knowingly send, save, view or access material containing content that may reasonably be considered threatening to any individual.
- 4.5.8 Actions or attempted actions to bypass, defeat or attack established City network, server, computer or any other security controls.
- 4.5.9 Unauthorized addition or modification to the City network, which includes, but is not limited to, the connection of personal or unauthorized network switches, routers, and wireless access points.
- 4.5.10 To read, delete, copy or modify Email of other users, without appropriate delegation or advanced authorization.
- 4.5.11 Any actions for the purpose of hacking, tampering, trespassing, probing, eavesdropping, monitoring, wiretapping, cracking, recording, breaching, surveying, intercepting, data theft, forgery, sabotage, spoofing (forgery of digital identity) of electronic communications and excessive loading or congesting (i.e., Denial of Service attack) of the City network or computers. This prohibition does not apply to legitimate investigations conducted by authorized persons or agencies in the collection of evidence.
- 4.5.12 To access or modify data or programs for which a user does not have authorization or explicit consent from the owner of the data/information, or from an appropriate level of management. (Refer to A.R. 90.64)
- 4.5.13 To knowingly introduce, distribute, propagate or download any computer viruses or other contaminants (e.g., computer worms or Trojans).
- 4.5.14 Accessing streaming audio or video or any other bandwidth intensive activities from Internet resources at any time for non-business use. Exceptions include streaming video from City of San Diego "City TV" as "City TV" is considered to be a work-related activity, and emerging technologies that may be used for City-related activities (e.g., posting of City communications on social media websites).
- 4.5.15 To download any software or applications from the Internet for personal use at any time, or for business use without proper advance approval from department management and the Department of IT.
- 4.5.16 To send or attempt to send "spam" messages (unsolicited Email messages, usually to a large number of recipients, including the sending of junk mail or other advertising material to individuals who did not specifically request such material), junk mail or any other for-profit messages, "chain letters" or any

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number	Issue	Page
INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE	90.62	2	5 of 7
	Effective Date December 7, 2012		

other mass mailings of a non-work related nature. (Refer to Administrative Regulation 90.65)

- 4.5.17 To forward Email or upload any file attachments containing confidential City data or information to a personal (external) Email account (e.g., Yahoo, AOL, etc.).
- 4.6 Individuals shall not disclose any of the City’s internal (i.e. proprietary or confidential) operations information on external (public or private) web logs (“blogs”), chat rooms, Internet forums, message boards, social media sites (Facebook, Twitter or YouTube) or other publicly accessible web sites, without the prior, written authorization from City management or City Council as required by policy or law. This does not apply to any information that is already publicly available from the City’s web site or other sites where the information was authorized to be posted.
- 4.7 The Department of IT is responsible for the development and management of the City’s public Web Site (www.sandiego.gov) and the City’s internal CityNet Web Site (citynet.sannet.gov). The Department of IT is the final authority for approving content from departments to ensure compliance with City Web Site guidelines and standards for appropriateness, style, structure, functionality, and accessibility, including compliance with the Americans with Disabilities Act.
- 4.8 City Departments shall use the City’s official public Web Site for all official City Internet postings. Social Media may only be used in accordance with the Social Media Guidelines available on Citynet (Located at Departments - Department of Information Technology – IT Services – Web Services – Web Policies & Procedures).
- 4.9 New Web Sites or Internet Domain Names shall not be obtained or created without the prior written approval of the Department of IT.

5. EMAIL POLICY

- 5.1 Email, and the electronic distribution of documents, is subject to all the same laws, policies and practices that apply to other means of communication, such as telephone and paper documents and records. This includes, but is not limited to, product endorsements, copyright laws, software licensing, patent laws, record retention, and proper business correspondence practices.
 - 5.1.1 Transmission of any material in violation of Local, State or Federal laws or regulations and City policy and procedures is prohibited.
 - 5.1.2 Under the California Public Records Act, any Email may be a public record. Individuals should be aware that electronic records are subject to the mandatory

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number	Issue	Page
INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE	90.62	2	6 of 7
Effective Date December 7, 2012			

public disclosure requirements of the Public Records Act, and subject to exceptions under the Act. Public Records Act requests should be handled in accordance with the City policy direction as stated in A.R. 95.20.

- 5.2 Individuals are responsible for all Email messages and attached documents originating from his/her user Email address and for directing Email only to intended recipients.

6. EMPLOYEE AND SUPERVISOR RESPONSIBILITIES

- 6.1 City IT Resources are provided for use in the pursuit of City business and are to be reviewed, monitored, and used only in that pursuit.
- 6.2 Each Individual is responsible for the content of all text, audio, or images that they place or send using City IT Resources.
- 6.3 Individuals who misuse City IT Resources are subject to disciplinary action up to and including termination.
- 6.4 The City may advise appropriate legal officials of any evidence of illegal activities. Individuals should contact their supervisor if they have any questions regarding appropriate use of City IT Resources.
- 6.5 Individuals accessing computers on the City network must acknowledge Acceptable Use prior to accessing City computers. City computers will prompt users for this acknowledgement prior to allowing access to the system.
- 6.6 Email and Internet/Web access are not entirely secure. Others outside the City may also be able to monitor Email and Internet/Web access. For example, Internet sites maintain logs of visits from users; these logs identify which particular person (based on Internet Protocol (IP) address) accessed the service. If an Individual's work requires a higher level of security, contact departmental IT staff or the Department of IT for guidance on securely exchanging Email or gathering secure information from sources such as the Internet or World Wide Web.
- 6.7 Individuals should safeguard the City's confidential information, as well as that of customers and others, from disclosure. Messages should be screened for confidential information prior to being viewed or shared with others. Messages containing confidential information should not be left visible while an individual is away from his or her work area. Department Directors should be engaged to provide guidance on confidential information and what security controls, if any, need to be applied to the information prior to being sent over Email.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number	Issue	Page
INFORMATION & COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE	90.62	2	7 of 7
Effective Date December 7, 2012			

APPENDIX

Legal References

San Diego City Charter Section 31

San Diego City Municipal Code Section 27.3654(b)

San Diego Administrative Regulation (AR) 45.50, "Private Use of City Labor, Equipment, Materials, and Supplies Prohibited"
AR 90.20, "Office and Wireless Telephones"
AR 90.63 "Information Security Policy"
AR 90.64, "Protection of Sensitive Information and Data"
AR 90.65, "Broadcast Email and Voice Mail"
AR 95.05, "Cell Phone and Other Handheld Communication Device Use Policy"

Subject Index

Information Technology
Acceptable Use – Information Technology & Communications
City Web Site, Acceptable Use
Computer Equipment, Acceptable Use
Communications Systems, Acceptable Use
Electronic Mail, Acceptable Use
Email, Acceptable Use
Network Services, Acceptable Use

Distribution

Department Heads
Department IT Administrators & Analysts
System Administrators

Administering Department

Department of Information Technology