



ADMINISTRATIVE POLICY

COMPUTER SYSTEM USE

City Manager
Andrew Pasmant

Please distribute to your staff and train them. If you have any questions, please call Tom Nguyen at x 8472.

RECEIVED
DEC 18 P4:27
WEST COVINA CITY MANAGER

1. **PURPOSE**

To establish a policy regarding the use of City's computer/network equipment, software and systems. This policy is incorporated by reference into the City of West Covina Employee Handbook. All affected Employees will receive a copy of this policy to be inserted in his or her Employee Handbook.

2. **DEFINITIONS**

- A. The term "Computer System" (the "System") shall mean all computers, hardware, software, and resources owned, leased, rented, or licensed by the City of West Covina ("City") which are made available for official use by City employees ("Employees").
- B. The term "Resources" shall include, but is not limited to, electronic mail ("e-mail"), the Internet, and such other similar software or applications available on the System.
- C. The term "Hardware" shall include, but is not limited to, computers, computer terminals, network equipment, modems or any other tangible computer device generally understood to comprise hardware.
- D. The term "Software" shall include, but is not limited to, all computer programs and applications other than the Resources available on the System.
- E. The term "Temporary or Permanent File" or "File" shall mean any electronic document, information or data residing or located, in whole or in part, on the System, including but not limited to spreadsheets, calendar entries, appointments, tasks, notes, or messages.

3. **OWNERSHIP**

The System, any Temporary or Permanent Files, and any related systems or devices are, and shall remain, the sole property of the City.

4. **SYSTEM INSPECTION OR REVIEW AND MONITORING**

An Employee's supervisor, with the approval of the Department Head, has the express authority to inspect or review the System, any and all Temporary or Permanent Files, and related electronic systems or devices and any contents thereof so long as such inspection or review is in the ordinary course of the supervisor's supervisory duties.

When requested by an Employee's supervisor, or during the course of regular duties requiring such information, a member(s) of the Information Systems staff ("IS") may extract, download, or otherwise obtain any and all Temporary or Permanent Files residing or located in or on the System.

Reasons for inspection or review may include, but are not limited to, System malfunctions, problems or general System failure, a lawsuit against the City involving the Employee or related to the Employee's duties, violation of a City policy, or a need to perform or provide a service when the Employee is unavailable.

THE CITY RESERVES THE RIGHT TO MONITOR THE SYSTEM FOR ANY REASON, INCLUDING THE RIGHT TO REVIEW, AUDIT AND DISCLOSE ALL MATTERS SENT OVER AND/OR STORED IN THE SYSTEM, IN ORDER TO ENSURE COMPLIANCE WITH THE LAW AND/OR THESE POLICIES.

5. UNAUTHORIZED DUPLICATION OF SOFTWARE

- A. Employees shall not copy or duplicate any copyrighted and/or licensed software except for a single copy for backup purposes. To reduce the risk of personal computer virus infection, Employees are not permitted to install personal copies of any software including, but not limited to "screen savers," onto the City's computers. If an Employee must copy data onto a disk and download it on a non-City computer, the Employee shall scan the disk for viruses before reloading the data on a City machine. Guidelines for this purpose shall be developed and distributed to all System users.
- B. No Employee shall knowingly make, acquire, or use unauthorized copies of computer software not licensed to the City on the System, or place or use unauthorized software on City premises or the System. Title 17 of the U.S. Code, Section 106, provides that unauthorized duplication of software is a federal offense. Both companies and individuals can be subject to civil damages of as much as \$100,000 per title copied, criminal penalties including fines (up to \$250,000 per work copied), and imprisonment (up to five years per title copied).

6. INTERNET USE

- A. Internet access shall be limited strictly to City-related business activities during Employees working hours. Personal use of the Internet will be permitted during scheduled breaks and non-working hours with the approval of the Department Head. Internet sites containing information that is not appropriate to the conducting of City business shall not be knowingly accessed by City employees through the System, including but not limited to adult forums, pornography, games, "chat rooms," and similar or related web sites.
- B. Information Systems Division tracks and monitors all Internet transactions by Employees using the Internet Management System; Department Heads have the right to request an Internet report of his or her staff for evaluation purposes.

- C. Information downloaded through the System shall be limited to messages, mail, and data files. No copyrighted and/or unlicensed software program files shall be downloaded through the System without prior approval of the Information Systems Division.
- D. Internet access by City Employees utilizing the City's access provider, Digital Island, shall conform to the standards agreed to between the City and Digital Island as a condition of the access agreement.
- E. All Employees using or accessing the Internet through the System hereby acknowledge the serious nature and existence of computer viruses. Employees shall be aware of their individual responsibility to protect the safety and security of the System. No Employee shall download files, material, or information from the Internet without using the proper virus-scanning program to protect the System from potential risk of, or infection from, such a virus.
- F. Employees shall report any unauthorized access to the System, or suspected intrusion from outside sources (including the Internet), to their Department Head and/or the Computer Systems Administrator.
- G. Internet access of Employees shall be limited to those Employees whose regular duties make Internet access necessary. Individual Employee access shall be determined, on a case-by-case basis, by the Department Head. The Department Head shall take into account factors such as the frequency, duration, and type of access needed by a particular Employee, and the extent to which such access is reasonably necessary to the regular duties of the Employee.

7. PROTECTION OF CITY SYSTEMS AND FILES

- A. All Employees have a duty to protect the System and related systems and devices from physical and environmental damage, and are also responsible for the correct use, operation, care, and maintenance of the System. Any City Employee with any questions, concerns or uncertainties about the correct use, operation, care and/or maintenance of the System should immediately directed to IS staff.
- B. All Employees shall use a City approved virus scan on all diskettes, files, documents, or other devices which are obtained from a source outside the City or from any non-City computer system.
- C. It is expressly prohibited for an Employee to allow an unauthorized user to access the System at any time or for any reason.
- D. Employees shall not intentionally use or develop any program that alters or damages the System, or which interferes with or disrupts the use of the System.

8. ELECTRONIC MAIL USE

- A. Employees who use electronic mail provided by the City are not guaranteed or warrantied any right of privacy. Messages may, in fact, be subject to disclosure under the provisions of the Public Records Act or for purposes of litigation. Any and all opinions stated or made using these Resources, whether implied or expressed, are those of the individual and not of the City of West Covina, its elected officials, or management.
- B. Allowable uses of the City's electronic mail include the following, to the extent that these uses are for the purpose of conducting City business:
 - 1. To facilitate performance of job functions.
 - 2. To facilitate the communication of information in a timely manner.
 - 3. To coordinate meetings of individuals, locations, and City resources.
 - 4. To communicate with departments throughout the City.
 - 5. To communicate with outside organizations as required in order to perform an employee's job functions.
 - 6. To conduct job related research.
 - 7. Occasional personal use on scheduled breaks and during non-working hours with the approval of the Department Head.
- C. Prohibited uses of the City's electronic mail includes, but may not limited to, the following:
 - 1. Illegal activities, including any activities which violate federal, State, or local laws, threats, harassments, slander, defamation, obscene, offensive pictures or graphic images, political opinions/endorsements, commercial activities, advertising, solicitation, or any otherwise inappropriate activity or activity that is unrelated to City business.
 - 2. Unauthorized reading/copying of the electronic mail of another Employee without prior written approval of the Employee's Department Head or the City Manager.
 - 3. The use of electronic mail to harass or annoy other Employees or anyone is explicitly and expressly prohibited at all times.
 - 4. Tampering, destruction or theft of others' electronic mail.
 - 5. Any other violation of this policy.
- D. An Employee's supervisor may have access to the contents of electronic mail pursuant to Section 4, "System Inspection or Review," of this Policy.

- E. Consult with supervisor or department heads before sending electronic mail to City Council or City Manager. The City Manager will need to approve any e-mails before they are sent to the City Council.

9. PASSWORDS / ACCESS CODES

For Systems and/or Files, which contain sensitive information, the use of passwords/access codes on the computer(s) and file(s) is encouraged. Whenever passwords/access codes are used, IS staff will by-pass and access all Systems and Files if requested and approval is received by all of the following: City Manager, Personnel and Police Departments. It is the Employee's responsibility to see that the password/access code information is kept current.

10. UNAUTHORIZED COMPUTER SYSTEM / FILE ACCESS

Except as provided in Section 4, Employees are prohibited from accessing computer Systems or Files unless they are authorized to do so in the normal course of City business.

11. VIOLATIONS OF POLICY

City Employees who violate this policy shall be subject to disciplinary action, up to and including termination.

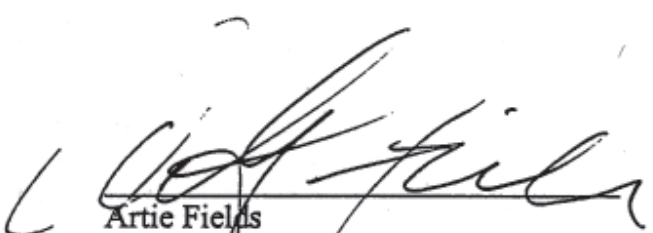
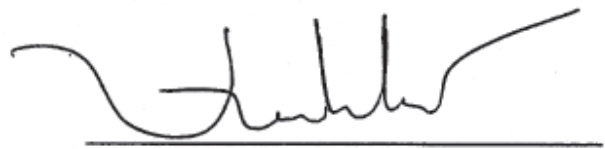
12. SUPPLEMENTAL GUIDELINES

Supplemental Guidelines on the interpretation and implementation of this policy may be distributed from time to time. These guidelines shall be incorporated by reference into this policy.

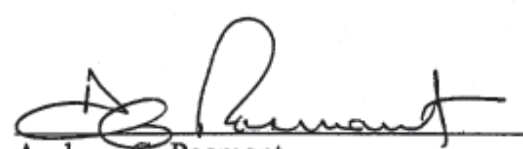
13. RETENTION OF ELECTRONIC MAIL

- A. The City and its Employees are required by law to retain all electronic mail that is an official public record. Any electronic mail that is part of official public business or is related to the formulation or implementation of policies and decisions would be considered an official public record. In order to retain these records, the Employee must print out the electronic mail message. The printed out hard copy shall be maintained in the appropriate City file. The original electronic mail message shall thereafter be deleted in the same manner as all other electronic mail messages.
- B. Drafts or any other documents not retained in the ordinary course of business are *not* official public records. In addition, copies of documents which are distributed for convenience or reference, and internal documents merely designed to further the flow of documents or information, such as cover notes, would not be considered official public records and do not need to be retained.

- C. If you have any question or concern about whether to retain a particular record, immediately contact your supervisor or Department Head *before* deleting the electronic mail message.
- D. Employees are to delete all electronic messages, including those that are required to be retained so long as the procedure for retaining a copy of that message are followed as set forth above, at least once a week, including messages in the Sent Mail folder.
- E. To ensure that the Deleted Mail folder is emptied each time a user signs out of Mail, the "Empty the Deleted Items Folder Upon Exiting" option is to be turned on in the Tools/Options/Other dialog box.
- F. Employees are recommended to keep paragraphs and messages short and to the point. Insert attachment if necessary.


Artie Fields
Acting Finance Director
Tom Nguyen
Computer Systems Administrator

TN/mn


Andrew G. Pasmant
City Manager

Immediately
Effective Date