CITY OF ROCKLIN

MEMORANDUM

DATE: August 8, 2003

TO: Department Heads
Division Managers

FROM: Judy LaPorte, Human Resources Manager

RE: Administrative Policy – Use of Electronic Communications

Per my recent email message, enclosed are copies of the above policy. Each copy has an acknowledgment page attached. You may make additional copies as necessary.

A copy of the policy should be given to all individuals with access to City provided systems. I encourage you to discuss the policy at a staff meeting. Please have the acknowledgment forms signed, collected and returned to Human Resources no later than August 25.

If you have any questions about the policy, please contact Rex Miller, Gary Cook or me. Thank you for your cooperation in ensuring that all individuals receive the policy and sign the acknowledgment form.

Acknowledgment of Receipt

Administrative Policy
Use of Electronic Communications
August 2003

I have read the City's "Use of Electronic Communications" Policy and agree to abide by the provisions of the policy.

Name (please print) _____

Signature _____

Date _____

Administrative Policy
Use of Electronic Communications

1. Purpose of Policy.

The purpose of this Administrative Policy ("Policy") for the Use of Electronic Communications is to provide guidance to City officers and employees ("Employees") regarding the proper and authorized use of the City's Electronic Communication Systems (including the E-Mail System) in accordance with the requirements of the "Public Records Act", as well as the requirements of the City's "Records Retention Policies."

If an Employee has any questions regarding the implementation of this Policy, contact either: the City Attorney's office (for legal questions, such as an interpretation under the Public Records Act); the City Clerk's office (regarding the Records Retention Policy); or the Information Systems division (regarding any technical issues related to the use of the Electronic Communications System).

2. Definitions.

As used in this Policy:

"Electronic Communication" means any communication or writing created by, retrieved by, sent to, or stored by any Employee using any Electronic Communication System, including all information, data, and attachments to the communication.

"Electronic Communication System" means the system of devices (including hardware, software, and other equipment) used by the City for the purpose of facilitating the transmission and storage of electronic information (including the E-Mail System, telephones, pagers, radios, computers, and all peripheral devices such as hard drives, disks, tapes, film, CDs, PDA's and handheld devices).

"E-Mail" means any Electronic Communication to or from any Employee using the E-Mail System, including all information, data, and attachments to the communication.

"E-Mail System" means the system of devices (including hardware, software, and other equipment) used by the City for the purpose of facilitating the electronic transmission of information, including Internet communications, and the City's Outlook Exchange system (including E-Mail, Calendar, and Tasks).

"Public Record" means, as defined by California Government Code section 6252(d), any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by the City regardless of physical form or characteristics.

"Public Records Act" means California Government Code sections 6200, *et seq.*

"Records Retention Policy" means the City's Records Retention and Disposition Policy as adopted in Resolution 92-019 and including any amendments.

"Writing" means, as defined by California Government Code section 6252(e), any handwriting, typewriting, printing, photostatting, photographing, and every other means of recording upon any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, magnetic or punched cards, discs, drums and other documents.

3. Policy.

3(a). Information on the Electronic Communication System is not private. The Electronic Communication System and all Electronic Communications are the property of the City. The City has the right, but not a duty, to inspect or audit any and all Electronic Communications, at any time, without notice to any Employee. Accordingly, no Employee shall have any expectation of privacy regarding the content of any Electronic Communications.

3(b). The Electronic Communications System shall be used in a professional manner. Employees shall prepare Electronic Communications in a lawful, ethical, professional, and businesslike manner. Employee's shall not use the E-Mail system for inappropriate communications such as, but not limited to: jokes, classified ads, editorials, discriminatory comments, profanity, pornography, etc. The use of the Electronic Communication System is a privilege, which may be revoked by the City at any time.

3(c)(1). Employees shall protect the security of the Electronic Communications System. Employees shall take all reasonable and necessary efforts to: protect the confidentiality of information which is placed in their control or care, minimize the likelihood of inadvertent transmission of confidential information to unintended recipients, prevent unauthorized intruders from accessing the Electronic Communications System, and prevent the introduction or spread of computer viruses. For the communication of sensitive and confidential information, Employees shall minimize the use of E-Mail and maximize the use of alternative communication media (such as face-to-face conversations, telephone, hard copy memos, and fax).

3(c)(2). Network Passwords. Each employee that has been granted access to the City's network shall be required to create an unique password. All passwords shall contain a minimum of eight characters, not be a word found in the dictionary and should contain non-letter characters such as numbers or symbols. Simple passwords are able to be "cracked" and divulged by simple internet hacking programs. If any employee suspects that their password has been compromised, they are to notify the Information Systems Division immediately. Employees shall protect their network password and not divulge them to anyone.

3(d). The Email System shall be used for transmission not storage. The E-Mail System is provided by the City to Employees as a convenient and efficient method of rapidly communicating transitory information in an electronic format. The E-Mail System is specifically intended and designed to be a tool for transmission of information, and not a tool for storage of information. The E-Mail System shall be automatically purged by the City pursuant to the schedule set forth in section 5(a) of this Policy.

3(e). If information from E-Mail is required to be retained, transfer the information from E-Mail to a records storage system. Since information on the E-Mail system is automatically purged, the City shall consider every E-Mail to be a preliminary draft (not retained in the ordinary course of business). However, if any information on the E-Mail System is required to be retained for the discharge of an Employee's duties (as described in section 5 of this Policy), the information shall be transferred from the E-Mail System to an appropriate records storage medium.

4. <u>Protect Confidential Information</u>.

Whenever an Employee possesses "confidential" information, the Employee has an obligation to take all reasonable and necessary steps to protect the confidentiality of the information, and minimize the likelihood of inadvertent transmission of the confidential information to unintended recipients. If an Employee has any question regarding the implementation of this section, contact the City Attorney's office.

4(a). Determine if the information is "confidential". Employees shall treat all information as "confidential" if there is any possibility that the information could be considered personal (such as personnel or medical records), or private (such as proprietary or financial information received from a third party), or if it could potentially expose the City to liability, or if it falls within one of the categories identified in section 6(d) of this Policy.

4(b). Identify the people who are authorized to receive the confidential information. Employees with the care and custody of confidential information shall be responsible for determining which other Employees (or possibly private attorneys or consultants hired to represent the City) are authorized recipients of the information. Generally, only people with a "need to know" the confidential information are authorized recipients. Employees with any questions as to who is an authorized recipient for confidential information shall contact the City Attorney's office. Do not communicate confidential information to any person other that an authorized recipient. **Do not forward a confidential E-Mail to any unauthorized recipient.**

4(c). Consider the availability of alternate means of communication. When it is necessary to communicate confidential information, Employees shall consider the risks and benefits of all available means of communication (including: face-to-face communications, telephone, E-Mail, fax, or hard copy memo), and Employees shall use a means of communication which minimizes the risk that the confidential communications will be received by an unintended recipient (that is, a person who does not "need to

know" the confidential information). For confidential information which is particularly sensitive (for example, highly personal medical information, or information which could expose the City to significant liability), Employees shall exercise a heightened sense of care in protecting the confidentiality of the information.

4(d). Minimize the use of E-Mail for confidential communications. For the communication of confidential information, Employees shall minimize the use of E-Mail and maximize the use of alternative communication media. In determining whether or not confidential information should be communicated via E-Mail versus some other form of communication, each Employee shall weigh the benefits of communicating via the E-Mail System (including, speed of communicating in writing over great distances, and the efficiency of electronic editing of documents by one or more people) against the risk that the confidential information may be inadvertently sent or forwarded to an unintended recipient.

4(e). Clearly identify all confidential writings. All confidential information which is contained in an Electronic Communication shall be clearly marked **CONFIDENTIAL**. If confidential information is required to be retained (as described below), it shall be clearly designated as **CONFIDENTIAL** in the appropriate storage or filing system.

5. Do Not Store Information on the E-Mail System.

The E-Mail System shall be used for the transmission of information, and shall not be used for the storage of information. If information on the E-Mail System is required to be retained for the discharge of an Employee's duties, the information shall be transferred to an appropriate records storage medium.

5(a). The E-Mail System will be automatically purged. All information on the E-Mail System shall be subject to automatic purging (that is, deletion) by the City, without any notice to Employees, in accordance with the schedule set forth below. However, unopened E-Mail messages will not be purged for 60 days.

> **5(a)(1).** The purge cycle for calendar, tasks, and notes shall be a rolling 365 day cycle. Each day, data that has been in the system for 366 days will be deleted.
>
> **5(a)(2).** Effective September 1, 2003, the purge cycle for "Received" E-Mail messages shall be 30 calendar days, the purge cycle for "Sent" messages shall be 30 calendar days, and the purge cycle for "Deleted" messages shall be 5 calendar days.

5(b). Determine if information on the E-Mail System is required to be retained. For each E-Mail sent or received, Employees shall determine whether or not there is information on the E-Mail which is required to be retained for the discharge of the Employee's official duties for the City. This determination shall be made using the same criteria which is applied to information sent or received by the Employee using any other means of communication. Employees with any question (as to whether a particular category of information is required to be retained) shall consult with their supervisor, and

supervisors shall consult with the City Attorney's office. Categories of information which are typically retained by the City include: (1) required by law to be retained; (2) documentation of notice to a member of the public of an action or position taken, or an action or position to be taken, on behalf of the City; (3) documentation of a City policy, City regulation, or official decision made on behalf of the City; or (4) documentation of the transaction of business between the City and another party.

5(c). Transfer required information from the E-Mail System to a records storage system. If an E-Mail contains information which is "required to be retained," as described above, the Employee shall: (1) transfer the required information from the E-Mail to an appropriate public record storage system (such as printing the E-Mail on paper) before it is deleted or purged from the E-Mail System, and (2) maintain the public record in accordance with the City's Records Retention Policy.

5(d). Do not bypass the automatic purge cycle. The "Archive" feature of the E-Mail System is not available for use as a record storage system. Employees shall not manipulate settings in the E-Mail System in an attempt to use the "Archive" feature or in an attempt to bypass the automatic purge cycle set by the City.

5(e). Delete all E-Mails. Since all E-Mails are preliminary drafts, every Employee (sending or receiving any E-Mail) shall delete the E-Mail as soon as the information is no longer required or convenient for the discharge of the Employee's duties, and the E-Mail shall be automatically purged by the City in accordance with the schedule set forth in this Policy.

6. Are E-Mails exempt from disclosure under the Public Records Act?

6(a). Are E-Mails Public Records? As indicated in the Definitions section, above, each and every E-Mail on the E-Mail System is a "Writing." Further, every "Writing" is a "Public Record" if it: (a) contains information relating to the conduct of the public's business, and (b) is prepared, owned, used, or retained by the City.[1] Since the primary purpose of the E-Mail System is to assist Employees in the conduct of City business (with the sole exception of occasional and limited "personal" use, described below), all such E-Mails are Public Records as long as they are retained by the City. Thus, although the City is authorized to delete "preliminary draft" E-Mails, until an E-Mail is actually deleted, the E-Mail is a Public Record if it contains information relating to the public's business.[2]

6(b). Are Public Records subject to disclosure to the public? Generally, all Public Records are open to inspection and copying by any person who makes a request in accordance with the requirements of the Public Records Act.

---

[1] Government Code section 6254(a).

[2] See the Public Records Ace, the City's Records Retention and Disposition Policy and Braun v. City of Taft (Polston) (1984) 154 Cal.App.3d 332, 201 Cal.Rptr. 654.

However, a Public Record may be exempt from disclosure if it falls within one of the categories of exemptions outlined below.

If an Employee receives a Public Records Act request for a document, which is potentially confidential or otherwise exempt from disclosure, the Employee shall contact the City Attorney's office.

6(c). Public records exempt as "preliminary drafts." A public record is exempt from disclosure under the Public Records Act if: (1) the writing is a preliminary draft, note, or memoranda, and (2) it is not retained by the City in the ordinary course of business, and (3) the public interest in withholding the record clearly outweighs the public interest in disclosure.[3]

> **6(c)(1). Definition of "preliminary drafts."** The City shall consider all E-Mails to be a preliminary draft, note, or memoranda, unless the information is required to be retained (as described in section 5(b) of this Policy).[4]
>
> **6(c)(2). Not retained in ordinary course of business.** No E-Mail shall be considered by the City to be retained in the ordinary course of business. As identified in this Policy, the E-Mail System shall be a tool for information transmittal, and it shall not be a tool for information storage. All information transmitted on the E-Mail System shall be subject to automatic purging in accordance with the schedule identified in section 5(a) of this Policy.
>
> **6(c)(3). Public Interest.** If an Employee receives a request from any person to inspect an E-Mail in accordance with the Public Records Act before the E-Mail is deleted, the Employee shall: (a) immediately notify the City Attorney, (b) segregate and temporarily preserve the requested E-Mail, and (c) maintain the confidentiality of the E-Mail until a determination is made by the City Attorney regarding the balancing of the competing public interests to withhold or disclose the E-Mail.

6(d). Public records exempt based upon confidentiality. There are many sources of legal authority to exempt a "confidential" public record from disclosure under the Public Records Act. It would be impractical to list all definitions of "confidential" records in this Policy; however, a list of the more commonly encountered confidential records is provided below. If there is any question as to whether or not a particular record is "confidential", contact the City Attorney.

> **6(d)(1). Personnel Records.**[5] This category of exemptions includes any "personnel, medical or similar files, the disclosure of which would cause an

---

[3] Government Code section 6254(a).

[4] See the Public Records Act, the City's Records Retention and Disposition Policy and Braun v. City of Taft (Polston) (1984) 154 Cal.App.3d 332, 201 Cal.Rptr. 654.

unwarranted invasion of personal privacy." However, employment contracts are not exempt.[6]

6(d)(2). Pending claims or litigation.[7] After a Government Code claim, or a lawsuit, has been filed against the City, the records "pertaining to" the claim or litigation become exempt until the claim or litigation is finally adjudicated or settled.

6(d)(3). Attorney/client privilege, and attorney work product.[8] As a general rule, it should be presumed that all communications from the City Attorney's office to a City employee are subject to the attorney/client privilege, and the communications should be protected accordingly.

6(d)(4). Police records and investigative reports.[9] This category of exemption includes a wide variety of issues including: portions of investigation reports, confidential informants, and firearm licenses.

6(d)(5). Feasibility studies for property acquisition or public contracts.[10] Unless required to disclose by eminent domain law, feasibility studies "relative to the acquisition of property, or to prospective public supply and construction contracts" are exempt "until all of the property has been acquired or all of the contract agreement obtained."

6(d)(6). Information obtained by the City in confidence.[11] Generally, proprietary information may be exempt from disclosure if: (a) the third party providing the information submits the information with the expressed intention to maintain the confidence, (b) the information has not previously been disclosed to others, and (c) the third party has a reasonable expectation that the information will be maintained in confidence based upon the manner by which the City obtained the information. Examples include financial information submitted as a condition of a license, certificate, or permit.

6(d)7. Public interest balancing test.[12] If a writing does not fit a specific category of exemption, the writing <u>may</u> still be exempt if: "on the facts of the particular case the public interest served by not making the record public clearly outweighs the public interest served by disclosure of the record." Typically, the public interest cited as justification for withholding records under this balancing

---

[5] Government Code section 6254(c) and (g); and Evidence Code sections 990-1007, 1010-1028, and 1035-1036.2

[6] Government Code section 6254.8.

[7] Government Code section 6254(b).

[8] Government Code section 6254(k) and Evidence Code sections 951-962

[9] Government Code section 6254(f), (k), and (u); and Evidence Code sections 1041, and 1043-1045.

[10] Government Code section 6254(h).

[11] Government Code sections 6254(e), (i), (k), (n), and 6254.6, 6254.7, 6254.9, 6254.15; Evidence Code sections 1040 and 1060-1063

[12] Government Code section 6255

test is the "interest in fostering robust agency debate" during the deliberative process.[13]

6(e). "Personal" Writings MAY not be Public Records. Occasional and limited "personal" use of the Electronic Communications System is allowed when the use does not: (1) interfere with the Employee's work performance, (2) interfere with the work performance of any other user, (3) have undue impact on the operation of the Electronic Communications System, or (4) violate any other provisions of this Policy, any other City policy, or legal requirement. Any such "personal" use of the Electronic Communications System may not be a public record, as long as it does not contain information relating to the conduct of the public's business. However, any such "personal" use is subject to inspection or audit by the City at any time, for any lawful purpose, without notice to any Employee. Accordingly, no Employee shall have any expectation of privacy regarding the content of any Electronic Communications. Additionally, the personal use of the Electronic Communications System is a privilege which may be revoked by the City at any time.

7. General Use of E-Mail System.

7(a). "All Employee" E-Mails. The E-Mail System is capable of simultaneously transmitting a message to All Employees on the E-Mail System, or all E-Mail users in a division or department. Full discretion must be exercised in determining when an All Employee or all department or division message is to be sent. If there is any question as to the appropriateness of an All Employee message, the approval of the sender's division manager must be obtained.

7(b). Do not attempt to disguise the origin of an E-Mail. No Employee shall attempt to disguise the origin of any E-Mail, unless authorized by the Chief of Police for a criminal investigation.

7(c). Do Not Access Other Employee's E-Mail. No employee shall access another Employees' E-Mail unless authorized by: (1) the other Employee, or (2) the other Employee's Department Head, or (3) as may be authorized in the conduct of an investigation for disciplinary and/or criminal actions.

7(d). Violations of this Policy. Violation of the Policy is subject to discipline up to and including termination.

7(e). Reporting criminal activity. Any Employee who discovers potential criminal activity involving the use of any Electronic Communication shall immediately report the activity to the Employee's Manager. The Manager shall immediately report the activity to the Police Chief and the Human Resource Manager.

---

[13] Citizens For A Better Environment v. California Dept. of Food and Agriculture (1985) 171 Cal.App.3d 704, 217 Cal.Rptr. 504.