MINUTES

MILWAUKIE CITY COUNCIL WORK SESSION
March 21, 2006

Council President Barnes called the work session to order at 5:30 p.m. in the City Hall Conference Room.

Council Present: Councilors Collette, Loomis, and Stone.

Staff Present: City Manager Mike Swanson, Community Development/Public Works Director Ken Asher, Resource and Economic Development Specialist Alex Campbell, Planning Director Katie Mangle, Community Services Director JoAnn Herrigel, Code Compliance Assistant Tim Salyers, Code Compliance Coordinator Les Hall, and Engineering Director Paul Shirey.

Introductions

Mr. Asher introduced Katie Mangle recently hired as the City's Planning Director.

Transportation Enhancement/Metropolitan Transportation Improvement Program (MTIP) Pre-application

Mr. Campbell discussed the two-year federal funding cycle. The Transportation Enhancement (TE) funds were administered by the Oregon Department of Transportation (ODOT), and Metropolitan Transportation Improvement Program (MTIP) was a regional pool of money. He discussed current conditions on 17th Avenue between downtown Milwaukie and Ochoco Street related to bike and pedestrian facilities, eroding sidewalks, and minimal bus stop amenities. Improvements would connect the bike/pedestrian route from the end of the 3 Bridges project through Sellwood where it would join with the east side trail system. Staff would bring an MTIP proposal to Council later this spring.

Councilor Stone asked what other projects were suggested for TE funds.

Mr. Campbell looked at other unfunded projects on the Capital Improvement Plan (CIP), and one of those was sidewalk on Logus Road. ODOT staff indicted 17th Avenue would be a much more competitive project. That project would require an intergovernmental agreement (IGA) with the City of Portland.

Councilor Stone asked if Portland would also be securing TE funds to complete its portion of the project.

Mr. Asher replied it would be structured in such as way that the entire project would be done either through a joint application or a side agreement with Portland.

Mr. Campbell added the City of Portland was doing work at 17th and Ochoco to fill the Sellwood Gap, and Milwaukie's project would complement that work.

Mr. Asher added the application would be competitive because both jurisdictions would be sponsoring it, and Metro and the region would like to see this piece connecting the regional assets. There were other ideas for funding the Logus Road project.

Councilor Collette noted there was a list of transportation projects prepared for the Clackamas County Coordinating Committee (C4), and she did not recall this project's being on the list. Milwaukie's list was substantial compared to some of the other jurisdictions.

Mr. Asher replied this project was more in the realm of bike/pedestrian deficiency issues, so it may not have been in the CIP as a high-priority road improvement as 17th Avenue flowed well for cars and buses.

Mr. Campbell commented this was the closest to a traditional project one could do with TE funds. Staff looked at the cost for doing both sides, and it would have been approximately $2 million. The east side of 17th Avenue under Milwaukie's jurisdiction had a steep drop off, so it would be very expensive to construct sidewalks and retaining walls. The thought was to install a two-sided bike lane and sidewalk on one side to keep down the costs. Sidewalks would not be included on the east side north of Milport. He noted that the mixed-use development would also help the application.

Councilor Loomis liked the idea of tying Riverfront Park to 3 Bridges, Springwater Corridor, Sellwood, and the Pioneer Cemetery.

Code Amendment Proposals

Mr. Hall discussed two proposed ordinance amendments for Council direction. The first dealt with meth labs. He proposed amending the nuisance section of the code by addressing properties deemed unfit for use due to illegal drug manufacturing. Currently, there were no provisions in the code for dealing with those types of properties, and fortunately there have been none to date. If one were found, the City could require that the property be boarded up, but the contaminants were still there. Under current rules, the structure could sit for up to six months before any action could be taken if the property owner had not done so. After that six-month period, the City or a citizen would have to bring suit against the property owner and have a judge fine to the point of abatement. That process could go on for quite some time. The city attorney and building official concur this type of ordinance would be appropriate in that the City could immediately contact the property owner and establish timelines for a quicker resolution. Clackamas County successfully uses a similar process.

Councilor Collette understood the property owner would be required to do the cleanup.

Mr. Hall said that was correct. The cost of cleanup could range from a few thousand to much more than that depending on how much of the property was declared unfit. If this occurred in an apartment, the City would go after the owner for cleanup of the area declared unfit that in the meantime could not be used. If the property owner refused to do the cleanup, the City would go through the municipal court process, charge the civil penalties, do the cleanup, and put a lien on the property for abatement costs.

Mr. Hall discussed the proposed ordinance regarding inoperable vehicles on private property. The current code addressed junk or dismantled vehicles but did not address those that were on properties for years that simply did not run. The proposed ordinance would close the loop. The code addressed where vehicles may be stored and did not allow them to be dismantled. However, it did not address those calls related to cars with flat tires and moss growing on them that did not move and were not project cars. The City can enforce on cars parked in the front yard, but people just move them into the driveway where they just sit. The neighborhood still has to look at them. The proposed ordinance would give people a time period, probably 15 days, in which to get the car fixed, and the program would provide flexibility to work with property owners as long as some progress was shown. The goal was compliance and not sending cases to court. There were a few places in the City where this was prevalent and cars had been sitting for years. At this time there was nothing code enforcement could do, and it was blight on the neighborhoods.

Councilor Collette asked if this applied to school buses.

Mr. Hall replied the ordinance would apply to any vehicle that was designed to transport people or goods including buses, trailers, and RVs.

Councilor Stone asked if the 15-day time period would be long enough to get a vehicle operable or to get it licensed.

Mr. Hall replied it should be sufficient time if someone was motivated. He had found from past experience that if people were not given deadlines, they did not get the work done. The department would work with people to extend deadlines if positive effort was shown.

Councilor Stone understood there were certain areas with difficulties. She asked how proactive the City would be in terms of contacting those people or would it be complaint-driven.

Mr. Hall said right now there were enough houses that the department knew about from complaints to keep busy for some time. He did not anticipate driving by and looking for expired tags. Often properties with these types of conditions had other things going on such as debris and he would to deal with multiple violations at one time. Code enforcement begins by sending out the first warning letter with a deadline for rectifying the problem. If nothing was done, then a second warning letter is sent. During that time people may call code enforcement and work something out. Ultimately, a citation was issued if there was no compliance.

Councilor Collette asked if there were places where people could store vehicles on their property. Some of her neighbors had an Airstream that they used as a guest room.

Mr. Hall said the City had code provisions regarding where vehicles may or may not be parked.

Citizens Utility Advisory Board Work Plan

Board members present: Chair Bob Hatz, Vice Chair Charles Bird, and Ed Miller.

Mr. Shirey said by practice over the past few years, the Citizens Utility Advisory Board (CUAB) has become an important checkpoint for the engineering department's projects and forwards recommendations to the Council. He reviewed the proposed work plan that included the street improvement funding program, 2007 – 2011 CIP, the two-utility system development charge (SDC), the wastewater master plan and future treatment, Johnson Creek Boulevard wastewater extension and annexation, well 8 replacement and Clackamas River Water (CRW) intertie agreement, and the stormwater code update.

Mr. Shirey discussed the wastewater treatment element and the citizens advisory committee (CAC). The City was responsible for the collection system, and the master plan addressed the needed capital for that part of the system. If the County was still spinning in regards to treatment, then the City would likely go ahead and adopt its plan until there was a better understanding of regional wastewater treatment. At that time he would recommend amending the SDC rates. He anticipated some direction from the County regarding treatment options later this year.

The Johnson Creek Boulevard wastewater extension and annexation had to do with unsewered properties north and south of the Johnson Creek facility. The County recently decided to create an urban renewal district to address infrastructure needs in that area. Milwaukie had been looking at a small area that included the Creek to the road and the property north of the offices to the County line. Some preliminary engineering and estimates have been done. Staff has started discussions with area residents and would continue to work toward the possibility that the community desired the service and was interested in annexation. The meeting with the residents was good, and there seemed to be more openness to the idea of the City's doing something good and on time.

The Board reviewed the Well 8 study results and would make a recommendation to the Council. Under the current terms of the agreement with CRW, the City was required to purchase a set amount of water whether the City needed it or not. The City was in the process of exploring its needs and production capabilities.

The City recently hired a stormwater engineer to work with onsite management of stormwater runoff. Staff would recommend adopting code similar to that of neighboring jurisdictions and looking at the private sector for more management to help the City meet clean water discharge standards. The code amendments would go before the Planning Commission and likely be ready for Council consideration in spring 2007.

Councilor Collette was impressed with the Board's work and felt it was a tremendous resource for the community.

Mr. Bird said Mr. Shirey was respectful of the Board's time, and the chair runs the meetings efficiently.

Councilor Stone said the work plan was very active. She had a question about the Board's charge. She had always thought that it worked on sewer, storm, and water matters and not really street infrastructure. She asked if that had changed.

Mr. Shirey said if one interpreted the code strictly, the number of things reviewed by the Board would be less. He made a more liberal interpretation to include the City's entire public infrastructure with the idea that broader was better.

Councilor Stone said several years ago the street improvement funding program surfaced. A group of citizens from different committees and the engineering department convened to discuss the topic. It had not popped out to her that the CUAB was in charge of streets, and it had involved a broader range of people.

Mr. Shirey did not think the Board was in charge of streets but rather served in an advisory position. If there were issues that needed more stakeholder input, then a process for public input would definitely be designed. There were traditional things that the CUAB considered such as rate setting, and there were other matters that benefited from the Board's input.

Mr. Swanson read from the code that outlined the Board's responsibilities that included reviewing utility rate structures and capital improvement programs, acting in an advisory capacity to the Council on those types of matters, and promoting public knowledge, understanding, acceptance and support of official utility programs proposed or implemented by the City.

Mr. Hatz added that the Board only met once a month, but Mr. Shirey did a lot of work during that month in preparing for the meetings.

Mr. Shirey acknowledged the Board's work and particularly Mr. Hatz who had been a member for about 12 years.

Councilor Loomis appreciated that everything that went before the Board was not rubberstamped and that issues were discussed civilly.

"Open Channel" Proposal

Councilor Barnes reported that the Mayor would like to discuss the proposal at a retreat as a team and incorporate most or all of it into the Communication Agreement.

Councilor Collette thought the idea of a retreat was good. She did not see anything on the surface of the proposal that the Council would disagree with but did not want to miss something when the Communication Agreement was discussed.

Councilor Stone thought it bore discussion and agreed to wait until everyone could participate. She thought from reading the documentation Mr. Swanson provided that every

thing covered the substance of the proposal. It was a matter of implementing and following an agreement; it did not matter how much paper there was.

Councilor Loomis agreed it was a matter of whether one was going to follow the rules or not. This proposal came to Council through the neighborhood leadership. It was his thought that it might help some people reflect more before they drifted away from the agreement. The sooner the better for the retreat.

Councilor Barnes concurred and asked that some possible dates be considered for a retreat to review the Council Communication Agreement, the Open Channels Proposal, and other items.

Regional Committee Assignments

Mr. Swanson gathered information on committees that sought members that were not City committees or commissions. When the North Clackamas Parks and Recreation District (NCPRD) was created in the early 1990's there were a number of neighborhoods designated with the City being its own neighborhood. The Commissioners appoint an Urban Parks Advisory Board (UPAB) member from each of those neighborhoods with specific terms. However, the term of the Milwaukie member was left up to the City. The current Milwaukie member has served for four years, and the term of office for the other neighborhoods was three years. He suggested the Council consider revisiting that particular appointment. The current representative had been active for the past four years, but it was probably time for a change.

Councilor Loomis noted it had always been a Council position in the past, but the Councilors did not attend. Because of that, the Milwaukie Park and Recreation Board (PARB) did not get any information, so one of the Board members started attending. He wished to put his hat in the ring for the position, as it was one that interested him. There were not a lot of positions where a Council member actually got to do something. He would speak with Mart Hughes to determine his ongoing interest.

Councilor Collette said there were other regional committees that were not on the list including the Economic Development Advisory Committee, the Public Safety Advisory Committee, and Library Board. Mayor Bernard had asked her if she was interested in taking over for him on a couple of things, but it would be difficult to make any assignments without him present. She suggested it be considered at the Council retreat, and the group agreed.

Councilor Stone asked that the list include the meeting times.

Councilor Loomis said in some cases the process was not followed as he found out when he attended a C4 meeting. If there were committees that Council members should be appointed to, then they should be apprised. It looked like there were only a couple like that

Councilor Stone asked for a list of staff that attended.

Mr. Swanson said there were some technical advisory committees that he would add. He noted that three of the finalists for the community development/public works director now worked at the Johnson Creek facility. It was a strong group of people.

Council President Barnes adjourned the work session at 6:31 p.m.

Pat DuVal

Pat DuVal, Recorder

AGENDA

MILWAUKIE CITY COUNCIL WORK SESSION
MARCH 21, 2006

MILWAUKIE CITY HALL
Second Floor Conference Room
10722 SE Main Street

WORK SESSION – 5:30 p.m.

A light dinner will be served.

Discussion Items:

	Time	Topic	Presenter
1.	5:30 p.m.	Transportation Enhancement and Metropolitan Transportation Improvement Program (MTIP) Flexible Funds	Kenny Asher/Alex Campbell
2.	5:45 p.m.	Code Amendment Proposals: • Clean-up Requirements for Properties Declared Unfit for Use • Inoperable Vehicles on Private Property	Les Hall
3.	6:00 p.m.	Citizens Utility Advisory Board Work Plan	CUAB Members & staff
4.	6:30 p.m.	"Open Channel" Proposal	Mayor Bernard
5.	6:40 p.m.	Regional Committee Assignments	Mike Swanson
6.	6:50 p.m.	Adjourn	

Public Notice

- The Council may vote in work session on non-legislative issues.
- The time listed for each discussion item is approximate. The actual time at which each item is considered may change due to the length of time devoted to the
- Executive Session: The Milwaukie City Council may go into Executive Session pursuant to ORS 192.660. All discussions are confidential and those present may disclose nothing from the Session. Representatives of the news media are allowed to attend Executive Sessions as provided by ORS 192.660(3) but must not disclose any information discussed. No Executive Session may be held for the purpose of taking any final action or making any final decision. Executive Sessions are closed to the public.
- For assistance/service per the Americans with Disabilities Act (ADA) please dial TDD (503) 786-7555.
- The Council requests that all pagers and cell phones be either set on silent mode or turned off during the meeting.

To: Mayor and City Council

Through: Mike Swanson, City Manager
Kenny Asher, Community Development and Public Works Director

From: Alex Campbell, Resource and Economic Development Specialist

Subject: Transportation Enhancement and MTIP/Regional Flexible Funds

Date: March 6, 2006 for March 21, 2006 Work Session

Action Requested

Direct staff to submit a pre-application for "Transportation Enhancement" funds to build bicycle and pedestrian improvements on 17th Ave. Staff wishes to update Council on the MTIP/Regional Flexible Funds process. Council direction will be sought in May as a more detailed recommendation is developed.

Background

Every two years the State of Oregon updates the federally-required State Transportation Improvement Program (STIP). The STIP is a list of all projects that are eligible for federal dollars. Each STIP covers four years of transportation projects; each cycle adds projects for the last two years of the STIP. The 2008-2011 STIP process is underway, and applications for projects to be built in 2010 or 2011 are due later this spring.

Two routes to inclusion in the STIP are the "Transportation Enhancement" (TE) Program and the Metropolitan Transportation Improvement Program (MTIP). TE is administered by ODOT, and applications are solicited from public and private entities on a statewide basis. MTIP is administered by Metro. The MTIP includes approximately $25 million per year in "regional flexible funds." Those regional flexible funds are awarded on a competitive application basis.

The TE program was created to fund projects to enhance the experience of transportation system users. While a great range of projects can meet TE requirements (e.g., historic preservation and archeological planning), any project must have a clear relation to surface transportation. A "notice of intent" to apply for TE funding is due March 23. Eligible projects include:

- Pedestrian and Bicycle Projects;
- Historic Preservation related to surface transportation;
- Landscaping and Scenic Beautification; and
- Environmental Mitigation (highway runoff and wildlife protection only).

Roughly $11 million in funding statewide is available for FY 2009 and 2010. Special consideration is given to projects that are in a "Special Transportation Area" (which would include McLoughlin Blvd. between River Rd. and Scott St.); or that support mixed-use development, tourism or economic development.

Metro has encouraged City of Milwaukie staff to consider applying for TE funds to provide bike lanes and sidewalk on 17th Avenue, between downtown and Ochoco Street. This would connect the Trolley Trail with the Three Bridges/Springwater Trail. The City of Portland has already secured funding to fill in the "Sellwood Gap," connecting the bike/ped route from the end of the Three Bridges project at SE 17th Ave. through to Sellwood where it can join with eastbank trail system. The 17th Avenue connection would fill another missing gap and greatly improve the overall system connectivity of these two major bike/ped facilities. Initial inquiries to TE project staff have indicated that such an application would likely compete well. The project would fall in the upper range of the size of projects that TE considers ($750,000+).

MTIP regional flexible funds are available for a wide range of projects and are allocated by JPACT, TPAC, and Metro council, with the assistance of Metro staff. Regional flexible funds project proposals are evaluated on both qualitative and quantitative bases. Key factors include a proposal's capacity to encourage economic development, relieve congestion, encourage alternative travel modes, support Metro's Region 2040 Land Use goals, and/or improve safety in a cost – effective manner.

The region is divided into four sub-areas (Clackamas, East Multnomah, Washington, and Portland), each of which are assigned a maximum for total requests. The Clackamas County sub-area has been instructed to make requests for no more than $15 million worth of total projects. At least 40% of regional flexible funds applications must be advanced under the CMAQ program. CMAQ stands for Congestion Mitigation/ Air Quality funds; to be eligible, projects must reduce auto trips and/or improve regional air quality.

The Clackamas “C-4” group will be coordinating applications from the sub-area to meet Metro’s instructions on overall request limits. Final applications are due June 30.

Concurrence

Planning, Community Services, and Engineering Departments have been consulted. Further coordination will be required as project selections are finalized and applications developed.

Fiscal Impact

TE projects require a 10% match. MTIP matches range from 10-30% of total project costs depending upon the type of project. The upper range of MTIP awards is $2-$3 million.

Work Load Impacts

This work will be absorbed into existing positions: chiefly the Community Development and Public Works Director and the Resource and Economic Development Specialist, with contributions from the departments of Engineering and Planning

Alternatives

Direct staff to not apply, or to apply for only 1 of the 2 programs.

Attachments

None

To: Mayor and City Council

Through: Mike Swanson, City Manager
JoAnn Herrigel, Community Services Director

From: Les Hall, Code Enforcement Coordinator

Subject: Amend Title 8 of Municipal Ordinance to include clean-up requirements for properties declared unfit for use.

Date: March 8, 2006

Action Requested

No action requested. This report is for informational purposes only. Staff seeks Council guidance.

Code Enforcement staff would like to amend Title 8 of the Milwaukie Municipal Code to insert section 8.04.070 (J) declaring houses deemed "unfit for use" due to the presence of hazardous substances/chemicals used in the manufacture of illegal drugs to be a nuisance affecting public health.

Background

Over the past several years there has been a dramatic increase in the use of methamphetamine, (meth). Meth can be easily created in almost any location. After a meth lab has been moved, or closed down by a law enforcement agency, the remaining chemicals or residue can create a substantial health risk to those that may become exposed to this residue.

Staff would like to amend the current code in order to address these issues should they arise. Important elements to any new code language would include:

- Encourages timely and proper clean up of contaminated sites.
- Specifically addresses properties used in manufacture of illegal drug manufacturing.
- Minimizes citizen exposure to hazardous substances.

Section 8.04.070 of the City's code lists nuisances affecting public health. This list does not currently list former drug labs. Thus, when and if a drug lab were identified in the City, the only recourse we have is to require a property, once vacated, to be boarded up according to our ordinance for vacant buildings. This would not address the issue of clean up of a house contaminated with chemicals from a meth lab.

Once a property has been determined to contain the makings of a lab, it is declared "unfit for use" by a law enforcement agency. After being declared unfit for use, the property is not to be used or occupied. However, there is no mechanism in place for immediate clean up. Properties may sit vacant for up to six months, during which time citizens still have the potential to become exposed to any remaining contaminants.

If the City were to change current code to address properties unfit for use, staff would, upon the property being declared unfit for use, be able to immediately notify the property owner and require that a certified contractor clean the property in a timely manner.

While there are currently no drug labs which have been declared unfit for use within the City of Milwaukie, there are several in the immediate area of the City. Staff feels that having our ordinance address this prior to such a discovery would give the City a procedure to address these issues.

Concurrence

Community Services, Code Enforcement and the Police Department feel that such a code amendment would be a benefit to the City, as it would allow for a speedy clean up of meth labs once the property has been declared unfit for use. Even if the property is not occupied, the potential of contamination still exists as children, pets, etc. may become exposed to the residue and spread the contaminants to other properties.

After speaking with the City Attorney, Gary Firestone, he agreed that the City should amend our current code to deal with the impacts of such a situation. Mr. Firestone feels that we may have some recourse under our current nuisance code, but additional language, specifically targeted towards unfit for use properties, due to illegal drug manufacturing, would give us a better alternative to deal with these types of situations.

The Police Department agrees that this would be beneficial to the residents of the City as it would allow the City to achieve clean up faster than it would be accomplished under current rules at the State level.

Fiscal Impact
The fiscal impact would be minimal, as we would use the same resources and procedures already in place to deal with violations of the City Ordinance.

Work Load Impacts
If this code change were to be approved and such a property were discovered within the City limits, the workload would be minimal, as we already have established procedures for violations of our nuisance code.

Alternatives
Do not change current code, leaving open the possibly of discovering a meth lab within the City and being unable to take action against the owners to clean it in a timely manner.

No change to current code and allow properties to remain unfit for use during the six-month period and bring suit against property owner after time has expired, with the possibility of property being used, or additional contamination occurring.

Attachments
Suggested language change amending Title 8 of Milwaukie Municipal Code.

ORDINANCE NO._____

AN ORDINANCE OF THE CITY OF MILWAUKIE, OREGON AMENDING CHAPTER 8.04.070 OF THE MILWAUKIE MUNICIPCAL CODE TO ADD PROPERTIES DECLARED "UNFIT FOR USE" DUE TO ILLEGAL DRUG MANUFACTURING CONTAMINATION TO THE LIST OF PUBLIC HEALTH NUISANCES.

WHEREAS, the City Council believes that properties that are declared "unfit for use" are detrimental to the public's health, safety, and welfare; and

WHEREAS, allowing properties that are unfit for use to remain in such a state increases the risk to the public's health safety, and welfare.

NOW, THEREFORE, THE CITY OF MILWAUKIE DOES ORDAIN AS FOLLOWS:

Section 1. Section 8.04.070 of the Milwaukie Municipal Code is amended to add a new subsection (J) to read as follows, with all other portions of Section 8.04.070 to remain in effect:

8.04.070 (J) Properties Declared "Unfit for Use"

(1) Property placed on the Oregon Health Division "unfit for use list" because it has been used for the manufacture of illegal drugs and that has not been issued a "Certificate of Fitness" by the Oregon Health Division.

Read for the first time on _____ and moved to a second reading by _____vote of the City Council.

Read the second time and adopted by the City Council on _____.

Signed by the Mayor this _____.

_____
Jim Bernard, Mayor

ATTEST:

APPROVED AS TO FORM:

Ramis, Crew Corrigan, LLP

_____
Pat DuVal, City Recorder

_____
City Attorney

To: Mayor and City Council

Through: Mike Swanson, City Manager
JoAnn Herrigel, Community Services Director

From: Les Hall, Code Enforcement Coordinator

Subject: Amend Title 8 of Municipal Code to address inoperable vehicles on private property

Date: March 8, 2006

Action Requested

No action requested. This report is for informational purposes only. Staff seeks Council guidance.

Code Enforcement staff would like to amend Title 8 of the City of Milwaukie Municipal Code to include the storage of inoperable vehicles on private property and to include a definition of inoperable vehicles in Title 8 definitions.

Background

Code Enforcement staff receives numerous complaints about vehicles that are in the driveway areas of houses, which are unlicensed, have flat tires, or are otherwise in a non-drivable condition being stored for extended periods of time. Currently, City Code only prohibits storage of vehicles that are dismantled or unlicensed in the front or side yard setbacks. The Zoning Ordinance states that "all vehicles, licensed or unlicensed, shall be stored in driveway areas only." Because many of the vehicles called in by complainants are not dismantled, they do not violate current code. They do, nonetheless detract from the livability and appearance of the neighborhood.

Staff would like to amend the code to gain better clarity and address the livability issues that current code language does not cover. In order to achieve this, staff would like to recommend the following changes:

1) Amend Title 8.04.070 (B) to include "inoperable vehicles" in the list of materials that are prohibited to be stored on private property.

2) Amend Title 8.04.010 – Definitions - to define “Inoperable vehicles” as: “any vehicle which has no current valid state vehicle license, or which cannot be moved without being repaired or dismantled or which is no longer usable for the purposes for which it was manufactured. This definition shall not include any vehicle kept in an enclosed building or any vehicle kept on the premises of a business lawfully engaged in wrecking, junking or repair of vehicles.”

Concurrence
Code Enforcement staff feels that this code change would be beneficial to the overall livability of neighborhoods.

Planning feels that an amendment of this type would be beneficial to the citizens of Milwaukie.

Fiscal Impact
Should such an amendment be approved, there would be no fiscal impact on the City. Non-compliance could cause abatements, which would be partially offset by penalties imposed by the Municipal Judge.

Work Load Impacts
This type of code change would cause a slight increase in enforcement action for Code Enforcement staff.

Alternatives
Make no changes and allow inoperable vehicles to continue being stored on private property.

Attachments
Suggested changes to code language in Title 8 of Milwaukie Municipal Code.

ORDINANCE NO. _____

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF MILWAUKIE, OREGON, AMENDING TITLE 8 OF THE MUNICIPAL CODE TO INCLUDE INOPERABLE VEHICLES AS A NUISANCE AND INCLUDE A DEFINITION OF INOPERABLE VEHICLES.

WHEREAS, the City recognizes the need to maintain neighborhood livability; and

WHEREAS, the parking of inoperable vehicles on private property detracts from the livability of neighborhoods; and

WHEREAS, inoperable vehicles create a nuisance and blemish the visual appeal of neighborhoods;

NOW, THEREFORE, THE CITY OF MILWAUKIE DOES ORDAIN AS FOLLOWS:

Section 1: Milwaukie Municipal Code Section 8.04.070(B) is amended to read as follows:

B. Debris on Private Property. Accumulations of debris, rubbish, manure, and junk, junk machinery or junk vehicles of any kind, inoperable vehicles, and other refuse located on private property that are not removed within a reasonable time and that affect the health, safety or welfare of the city;

Section 2: Milwaukie Municipal Code Section 8.04.010 is amended to read as follows:

8.04.010 Definitions.

Except where the context indicates otherwise, the singular number includes the plural and the masculine gender includes the feminine, and the following definitions shall apply:

A. “City” means the City of Milwaukie.

B. “City manager” means the city manager or person authorized by the city manager.

C. “Council” means the governing body of the city.

D. “Inoperable vehicle” means any vehicle which has no current valid state vehicle license, or which cannot be moved without being repaired or dismantled, or which is no longer usable for the purposes for which it was manufactured, and which has been in that condition for at least 15 days. “Inoperable vehicle” does not include any vehicle kept on an enclosed building or any vehicle kept on the premises of a business lawfully engaged in wrecking, junking or repair of vehicles.

E. “Person” means a natural person, firm, partnership, association or corporation.

F. “Person in charge of property” means an agent, occupant, lessee, contract purchaser or person, other than the owner, having possession or control of the property.

G. “Public place” means a building, place or accommodation, whether publicly or privately owned, open and available to the general public.

Read the first time on _____ and moved to second reading by _____ vote of the City Council.

Read the second time and adopted by the City Council on _____.

Signed by the Mayor on _____

_____
Jim Bernard, Mayor

ATTEST:

Pat DuVal, City Recorder

APPROVED AS TO FORM:

Ramis, Crew, & Corrigan, LLP

_____
City Attorney

To: Mayor and City Council

Through: Mike Swanson, City Manager
Kenneth Asher, Dir. of Community Development & Public Works

From: Paul Shirey, Engineering Director

Subject: Citizen Utility Advisory Board (CUAB) Work Plan for 2006

Date: March 6 for March 21, 2006 Work Session

Action Requested

No action needed. For information purposes.

Background

Milwaukie code requires that advisory boards seek City Council endorsement of annual work plans. The Engineering Department provides the CUAB with staff support.

This work session provides Council with an opportunity to provide feedback and input on these important projects and programs.

The CUAB/Engineering work plan (**see Attachment**) for 2006/07 includes:

- **Street improvement funding program**: this will define street system needs; explore methods of funding needed improvements and engaging the community in a discussion to determine the public's willingness to invest in those improvements.
- **2007-2011 CIP**: develop and comment on proposed five-year capital improvement program and recommend approval of projects and funding levels for 2006/07 budget.
- **Two-utility SDC program update**: review the update of the System Development Charge (SDC) for water and stormwater based on latest master plans.

- **Wastewater Master plan and future of wastewater treatment** in N. Clackamas County: incorporate results of the County's wastewater treatment plan into Milwaukie wastewater master plan.
- **Johnson Cr. Blvd wastewater extension and annexation project**: develop plans and costs for extending treatment services and facilitate annexation of property owners wishing to connect to sewer.
- **Well 8 replacement and Clackamas River Water agreement**: analyze the cost of drilling a new well at site #8, or purchase additional water from Clackamas River Water.
- **Stormwater code update project**: consider revisions to Milwaukie code for new water quality standards for management of on-site storm water.

Concurrence

Operations, Planning, Finance and Community Services are aware of these projects and are or will be engaged as part of the implementation team on some or all of the projects.

Fiscal Impact

None

Work Load Impacts

All the projects in the CUAB work plan are included in the Engineering work plan.

Alternatives

Modify the proposed work plan.

Attachments

CUAB/Engineering Workplan 2006/07

CUAB/Engineering Department Work Plan 2006/2007

Item	Definition	Status	Complete Date
1. Street improvement funding program	Explore options for defining needed street improvements using Pavement Management System (PMS). Develop funding alternatives to pay for improvements. Engage the community in a process to determine what level of improvements, if any, will be funded.	Engineering to form a work team to define needed improvements and explore funding options for consideration by Council by June.	June '06:Return to Council with project lists, costs and funding alternatives. July/Aug: meet with community interests Sept: forward recommendations to Council.
2. 2007-2011 CIP	Review and make recommen-dations to Council on the Capital Improvement Plan for next 5 years. Make recom-mendations to City Council.	Final draft due for first Budget Comm. meeting Apr 11, '06.	Present to CUAB April 2006; forward to Budget Committee April; City Council May 2006.
3. Two-Utility SDC update	Complete work on 2-utility SDC (water & storm) update by April 2005. Wastewater pending outcome of County process in Oct '06.	Pursuant to state law, notice of intent published on Dec 31, '05. Methodology available on 2/16/06. Hearing to adopt revisions 4/18/06	CUAB review on April 5, 2006. Council hearing to adopt on 4/18/06.
4. Wastewater Master Plan & future of wastewater treatment in Clackamas County	Update Master Plan to define capital needs for wastewater collection utility and define needs for wastewater treatment.	Master plan for collection system completed and endorsed by CUAB Jan '06. Plan adoption deferred pending County implementation of wastewater treatment plan (Clearwater).	ON HOLD. Plan must reflect decision of County regarding treatment plans, expected in Fall '06.
5. Johnson Cr. Blvd. wastewater extension and annexation project	Boundaries include un-sewered areas north/south of JC offices; extension estimate prepared; seeking funding alternatives in addition to CDBG.	Outreach to community will determine project political feasibility.	Outreach: Mar/Apr '06.
6. Well 8 replacement and CRW inter-tie agreement	Analyze cost to drill replacement well on site #8 and determine least cost alternative for City to remain self sufficient, i.e.: does city need CRW source?	Well 8-replacement alternatives study completed.	Work session with Council Apr. '06
7. Stormwater code update project	Consider revisions to Milwaukie code for new water quality standards for management of on-site storm runoff.	Develop work plan and schedule; explore other jurisdictions requirements; develop scope for outside technical assistance.	Revisions to CUAB in Sept; Planning Comm. in December and CC in Feb. 07

TO: **MAYOR AND CITY COUNCIL**
FROM: **MIKE SWANSON, CITY MANAGER**
DATE: **FEBRUARY 23, 2006 FOR MARCH 7, 2006 WORK SESSION**
RE: **ATTACHED "OPEN CHANNEL" PROPOSAL**

ACTION REQUESTED

The action requested is direction from the Council on how to proceed with the "Open Channel" proposal.

BACKGROUND

Greg Chaimov developed the attached proposal, and the NDA Chairs at their January meeting recommended it for approval. Mayor Bernard forwarded it to me and requested that it be brought before Council for discussion. One approach suggested is that the principles be included in the Council Communication Agreement.

To assist in your consideration, I have attached a copy of a number of statements regarding communication between Council members and between Council and staff. They are:

- Milwaukie City Charter, Section 27(f);
- Milwaukie Municipal Code, Section 2.04.390;
- Council Communication Agreement; and
- Council Contact Memo dated September 27, 2000.

OPEN CHANNELS INITIATIVE

(1) "Public official" means a city councilor or the mayor.

(2) If a public official communicates with a city employee about the substance of a matter that will come before the council, the public official shall, if reasonably feasible, communicate with the employee through electronic mail, showing copies at the time of transmission to the other public officials and, if the employee is not the city manager, to the city manager. If the communication with the employee did not occur through electronic mail, the public official shall inform the other public officials of the substance of the communication before the council votes on the matter.

(3) Before the commencement of a meeting at which the council will vote on a matter, a public official shall make a reasonable effort to learn the other public officials' views on the matter by communicating directly with the other public officials.

(4) The mayor shall:

(a) Meet with the city manager at least once a week to discuss matters that will come before the council; and

(b) Unless the mayor considers maintaining the confidentiality of the discussion necessary to ensure full and frank communication with the city manager, within one working day of the meeting, inform the other public officials of the substance of the meeting.

(5) A public official may not impugn the integrity, impartiality, or competence of a city employee or another public official.

(6) A public official shall actively seek to improve communications with other public officials.

Milwaukie City Charter, Section 27(f)

INTERFERENCE IN ADMINISTRATION. No member of the council shall directly or indirectly, by suggestion or otherwise, attempt to influence or coerce the manager in the making of any appointment or removal of any officer or employee or in the purchase of supplies; or attempt to extract any promise relative to any appointment from any candidate for manager; or discuss directly or indirectly with him the matter of specific appointments to any city office or employment. Nothing in this section shall be construed, however, as prohibiting the council from fully and freely discussing with or suggesting to the manager anything pertaining to city affairs or the best interests of the city.

Milwaukie Municipal Code, Section 2.04.390

Councilors shall respect the separation between policy-making and administration by:

A. Not attempting to influence or coerce the city manager concerning personnel or purchasing, as outlined in Section 27(f) of the City Charter;

B. Addressing all inquiries and requests for information from staff to the city manager or city attorney and allowing sufficient time for response. At the discretion of the manager or attorney, inquiries may be forwarded to the full council for consideration;

C. Limiting individual contacts with city officers and employees so as not to influence staff decisions or recommendations, undermine the authority of supervisors or prevent the full council from having the benefit of any information received;

D. Honoring the confidentiality of discussions with the city attorney;

E. Attempting to work together with the staff as a team in a spirit of mutual confidence and support. (Ord. 1812 § 12, 1996; Ord. 1480 § 9(A), 1981)

MAYOR/COUNCIL COMMUNICATION AGREEMENT

Guaranteed access to clear and easily understood information is a value of the City of Milwaukie. These agreements are intended both to foster conduct that realizes that value, while ensuring a healthy debate about competing ideas. Finally, they seek closure and a community that moves forward together, secure in the knowledge that decisions were made openly and fairly.

The agreements have one common behavioral thread—mutual respect. Thus, if the list does not anticipate a situation, a response that is respectful of all concerned should suffice.

1. In all Council events, work sessions, and meetings:
   - I demonstrate respect for all who are involved;
   - I respect all thoughts and ideas;
   - I clarify facts and opinions to ensure understanding;
   - I do not personalize my comments;
   - I clearly state my own opinion as being mine;
   - I look for ways to praise efforts and accomplishments; and
   - I stay focused and participate.

2. In working with the Mayor and Councilors:
   - I provide them with reasonable notice of matters I am introducing at meetings;
   - I always represent the City's position before other jurisdictions unless none has been adopted, in which case I inform the Mayor and Council in a timely manner of the position(s) I have taken;
   - I work toward consensus;
   - Once the group has acted, I accept and respect the decision, and I do not publicly ridicule the Council, any individual member or participant, or the decision; and
   - I first address a concern about either a violation of these agreements or any other matter in a direct, appropriate, private, and timely manner.

3. In working to seek broad-based community support:
   - I communicate with the community to gather information; and
   - I engage the community in a shared dialogue.

4. In working with staff:
   - I communicate with staff to gather information; and
   - I exchange ideas with staff and give direction through the City Manager with the concurrence of the Mayor and Council.

James Bernard, Mayor

Deborah Barnes, Council President

Carlotta Collette, Councilor

Joe Loomis, Councilor

Susan Stone, Councilor

To: Milwaukie Management Staff
FROM: Mike Swanson
DATE: September 27, 2000
RE: Council Contact

The purpose of this memo is to clarify my expectations with regard to contact with individual Council members.

My authority for promulgating these guidelines can be found at Section 27(c)(3) of the Milwaukie Charter as follows:

> Shall appoint all city officers and employees and remove them, except as otherwise provided by this charter, *and have general supervision and control over them and their work* with power to transfer an employee from one department to another *and shall exercise supervision and control over the departments to the end of obtaining the utmost efficiency in each of said departments* . . . . (Emphasis mine.)

My general policy is to encourage the free flow of information between Council and staff in order to ensure that the Council receives the information to enable them to discharge their responsibilities. (I also expect that the same general policy applies to your staff with regard to communications with me.)

Within that general framework, however, are the following caveats:

- Council communications are to be initiated by Council members;
- Do not use the opportunity to criticize or otherwise undercut another staff member or City department. (If you have issues or concerns of this nature, the discussion should be between you and your immediate supervisor);
- If a Council member requests that you take action, do not argue about the propriety of taking action based on the request of one Councilor. Rather, acknowledge the request and discuss it with your immediate supervisor;
- Under no circumstances are you or your staff to discuss either personnel actions (such as disciplinary matters) or collective bargaining;
- "Political" issues should not be discussed nor advice given in one's role as an employee;
- If asked about a staff recommendation before the Council, answer truthfully but inform the manager and/or staff member making the recommendation in a timely manner. (The purpose is not to hold everyone to a "party line," but, rather, to ensure that the person(s) making the recommendation is not surprised.)
- Council/staff communications should be reported to one's supervisor again to ensure that there are no surprises.

Once more, I believe that the free flow of accurate, constructive, and responsible information will lead to credible results. To that end it is my desire that Council/staff communications be sanctioned, subject to the above guidelines. If you have any questions about any of the above or a specific situation, please do not hesitate to contact me.

Introduction

This manual was developed under the auspices of the Oregon State Archives and the Oregon Association of Municipal Recorders (OAMR) Records Management Committee (RMC) as a tool to help local government agencies answer the following types of questions related to e-mail:

- Do I have to print all e-mails?
- How long do I have to keep them?
- What about junk e-mail? Can't I just delete them?
- How should I handle work-related e-mail that is sent from a personal account?
- Does a public records request mean that I am responsible for producing copies of any and all e-mail messages I have received?
- Do city councilors and county commissioners have to follow the agency e-mail policy?
- Does training on the e-mail policy need to be provided?
- How should the e-mail policy be enforced?

Many users have come to rely on e-mail as a convenient and efficient communication tool. Oregon's Public Records Law applies to e-mail in state and local government agencies, requiring them to treat e-mail in the same manner as the other important business records of their office. By preserving information for as long as it is needed in order to document business functions, agencies can reduce their risks of litigation and loss of important information.

The following chapters should be helpful to anyone who uses e-mail in the course of business:

Chapter 1: Public Records Issues
Chapter 2: Writing a Policy
(a) Use
(b) Access
(c) Retention
(d) Training/audit
Chapter 3: Retention/Disposition/Filing
Chapter 4: Security
Chapter 5: Technology
Chapter 6: Budget
Chapter 7: Netiquette
APPENDIX
A. Glossary
B. Templates
C. Training

By using the suggestions presented in this manual, you should be able to meet any administrative and/or legal challenges regarding the access to and retention of e-mail messages. There is no one-size-fits-all solution to e-mail management issues, but the advice contained in this manual can help any agency begin to meet their responsibilities for managing e-mail.

Using this Manual

This manual is designed to help you take control of the e-mail records in your office. The chapters that follow are organized to allow easy access to the specific information about that topic. Each chapter provides an introduction that describes the purpose of that section; a case study to provide examples of applying the information to the workplace; and a short quiz at the end of each section to assist users in thinking about the issues that have been presented. Chapters also provide valuable links to additional resources and works that have been cited. Following those links will lead to websites that provide further explanation and information. The manual can be printed and used in a traditional manner (pdf version) or used electronically as an interactive guide and tutorial.

The electronic version includes narrated PowerPoint slide shows for each chapter providing examples and further explanations on a particular topic. In addition, the online version provides hyperlinks to the glossary for standardized definitions of terms relating to e-mail and e-mail management. For example whenever you see the word “e-mail” it will appears as underlined and in a different color (i.e. e-mail). When you click on the word, you will be taken to its definition in the glossary.

A short, introductory video, illustrating the need for a formal plan for managing your e-mail, is also included as part of this training.

Therefore, it is up to you to decide just how much information you need to manage your e-mail effectively. So start at the beginning or jump straight to the section you need most. Either way, if your organization needs an effective approach for managing its e-mail, then this manual should prove to be a valuable tool.

Chapter 1
Public Records Issues

Purpose

The purpose of this chapter is to familiarize employees with the Oregon Public Records Law (ORS 192) in relation to both access and retention. A clear understanding of the law should eliminate many of the questions and misunderstandings that staff may have with e-mail messages as public records.

It is important for all local government employees to be aware that an e-mail message may be a public record for both access and retention purposes. In our quest for efficiency, we use computers to communicate with each other and with our constituents. This kind of communication may put us at risk of violating Oregon's open government laws, specifically the public records and open meeting laws. These laws were adopted to ensure that the government process remains open to the public.

The Oregon Public Records Law

The Oregon Public Records Law was enacted by the Oregon Legislative Assembly in 1973. The law is divided into two parts. The first part relates to the retention and disposition of public Records. ORS 192.105 authorizes the State Archivist to grant public officials authorization for the retention and/or disposition of public records in their custody, after the records have been in existence for a specified period of time. In granting such authorization, the State Archivist shall consider the value of the public records for legal, administrative or research purposes and shall establish rules for procedure for the retention or disposition of the public records.

The second part of the law, ORS 192.420 establishes "every persons" right to inspect any nonexempt public record of a public body. ORS 192.501 conditionally exempts certain records from disclosure "unless the public interest requires disclosure in the particular instance." Very few records, in Oregon, are exempt from disclosure.

Oregon's Public Records Law applies to all public entities in the state, but does not apply to private entities or private bodies such as nonprofit corporations or cooperatives. The law requires the custodian of public records (i.e. a city) to provide "proper and reasonable opportunities for inspection and examination of the public records during usual business hours." The law further requires that persons inspecting records be provided with "reasonable facilities" for reviewing records.

Public Records Defined

The definition of public record in Oregon is also defined according to its relationship with retention and disposition and its relationship to access.

ORS 192.005 (5) defines a public records for retention and disposition purposes:

> "Public record" includes, but is not limited to, a document, book, paper, photograph, file, sound recording or machine readable electronic record, regardless of physical form or characteristics, made, received, filed or recorded in pursuance of law or in connection with the transaction of public business, whether or not confidential or restricted in use.

ORS 192.410(4) defines a "public record" as it relates to access:

> "…any writing containing information relating to the conduct of the public's business, including but not limited to, court records, mortgages and deed records, prepared, owned, used or retained by a public body regardless of physical form or characteristics."

Both definitions include information stored on computer tape, microfiche, photographs, film, tape or videotape, maps, files or electronic recordings that may be in "machine readable or electronic form."

However, purely personal messages, as well as unsolicited messages and advertisements (spam), are not public records under the retention/disposition aspect of the law but may be accessible to the public under the access portion of the law. Therefore, it is imperative that your agency's written e-mail policy clearly defines appropriate use of your e-mail system and individual e-mail accounts.

In addition, work done on private e-mail accounts as well as personally purchased computers and hand held devices might be considered a public record for both access and retention/disposition. It is strongly recommended that elected officials use a designated account for official business and that the policy prohibits official business from being conducted by Instant Messaging or Chat Rooms unless there is a specific mechanism in place to capture this information. It is also important for agencies to provide training on public records issues for elected officials, board and commission members, and employees.

Finally, records need not have been prepared originally by the public body to qualify as public records. If records prepared outside the agency contain information relating to the conduct of the public's business and are "owned, used or retained" by the public body, the records are within the scope of the Oregon Public Records Law.

Public Records Retention

A record that fits the definition of a public record will also have a retention requirement—that is, how long shall this information be retained to satisfy the administrative, legal, fiscal and/or historical needs of an agency. The State Archives works with state and local government agencies to determine the proper amount of time (i.e. 3 years) a particular record needs to be kept. These "retention schedules" are your legal authority to dispose of public records and can be obtained through your City Recorder, County Clerk, agency records officer or by contacting the State Archives. However, since e-mail is a method or a tool for communicating, a blanket retention for "E-mail Records" does not exist. Therefore each message needs to be evaluated for content to determine which retention to apply. Retention of e-mail messages is covered in more detail in Chapter 3.

Charging for Records Requests

The Oregon Public Records Law expressly authorizes a public body to establish fees "reasonably calculated to reimburse it for its actual cost in making such records available." It further permits local government to include in its fees "costs for summarizing, compiling or tailoring a record to meet the person's request." "Actual cost" may include a charge for the time spent by staff to locate the requested records, review the records to delete exempt material, supervise a person's inspection of the original documents in order to protect the records, copy records, certify documents as true copies or send records by special methods such as express mail. It also includes the cost of an

attorney reviewing and segregating records that should not be disclosed.
It is strongly recommended that local governments establish a fee schedule and written policy on public information/records requests and have the policy reviewed by legal counsel and adopted by the commissioners or councilors.

What is exempt from disclosure?
The Oregon Public Records Law is primarily a *disclosure* law, rather than a confidentiality law. The law generally favors the public's interest in access to government records, rather than the government's interest in confidentiality. A public body that denies a records inspection request has the burden of proving that the record is exempt from disclosure. Exemptions do not prohibit disclosure and most exemptions are conditional; disclosure is more often favored. The policy underlying the conditional exemption statutes is that disclosure decisions should be based on balancing those public interests that favor disclosure of governmental records against those public interests that favor governmental confidentiality, *with the presumption always being in favor of disclosure*. ORS 192.501 contains a list of "conditionally exempted" records.

The 'Why Not' Approach (LOCal Focus/September 2002)
Rather than viewing requests as adversarial, consider adopting a "Why not?" approach. When faced with any request ask yourself three questions:

1. Does federal or state law prohibit us from disclosing this information (i.e. would we be violating an employee's right to privacy by disclosure)?

2. If there is no prohibition, does Oregon law provide an exemption from disclosure?

3. Even if there is an exemption, should we disclose anyway?

In many cases, disclosure will only improve community relations and will serve to keep the government process open. After examining the request (with the assistance of your legal counsel), you may realize that no harm will be done by disclosure.
Many government employees may not be aware that information stored on their computer is subject to public disclosure. Informing your staff about Oregon's public records laws is the first step to ensuring that your agency complies with both the letter and the spirit of the law.

For more information….
To become more knowledgeable about the Public Records Law, all City Recorders, County Clerks and agency records officers are strongly encouraged to obtain a copy of the Attorney General's Public Records and Meetings Manual. This manual is an *excellent* resource for anyone responsible for public information/records requests. The manual may be purchased for a small fee from:

Department of Justice
Administrative Services Department
1175 Court Street NE
Salem, OR 97310
Phone: 503-378-5555

Chapter 1 - Case Study

Jane Allen submits a request for all City Council records relating to a particular zoning dispute. City Council members discussed the dispute in City Council meetings. In addition, several City Council members discussed the issue via Instant Messaging programs and in online chat rooms. Under Oregon's Public Records Law and Public Meetings Law, what records must be produced to satisfy Ms. Allen's request?

Oregon's Public Records Law has been interpreted very broadly. Subject to the exemptions and conditions of the Law, any covered documentation, whether in paper, electronic, or other format, can be considered a public record, which means that it must be retained according to records retention schedules and produced when requested. In addition, Oregon's Public Meetings Law applies to all government entities in Oregon. The Public Meetings Law covers City Councils. The Public Meetings Law defines a meeting as the convening of an Oregon government entity "for which a quorum is required in order to make a decision or to deliberate toward a decision on any matter." (ORS 192.610(5)) The requirements for a quorum can be met at a City Council meeting or in any electronic forum. All records of conversations or discussions of the quorum, including paper records, e-mail messages, or transcripts of on-line chats, are considered public records for the purposes of access and retention.

Chapter 1 - Quiz

1. **Is every e-mail message considered a public record?**
   Only messages sent, received, filed or recorded in "pursuance of law or in connection with the transaction of public business, whether or not confidential or restricted in use are considered public records" under ORS 192.005 (5) for retention and disposition purposes. However, purely personal messages, as well as unsolicited messages and advertisements (spam), are not public records under the retention/disposition aspect of the law but may be accessible to the public under the access portion of the law (ORS 192.410(4)).

2. **What e-mail messages are exempt from disclosure as public records?**
   The Oregon Public Records Law is primarily a disclosure law, rather than a confidentiality law. The law generally favors the public's interest in access to government records, rather than the government's interest in confidentiality. A public body that denies a records inspection request has the burden of proving that the record is exempt from disclosure. Exemptions do not prohibit disclosure and most exemptions are conditional; disclosure is more often favored. The policy underlying the conditional exemption statutes is that disclosure decisions should be based on balancing those public interests that favor disclosure of governmental records against those public interests that favor governmental confidentiality, with the presumption always being in favor of disclosure. ORS 192.501 contains a list of "conditionally exempted" records.

3. **What should a city consider when establishing a fee schedule for an e-mail request?**
   The Oregon Public Records Law expressly authorizes a public body to establish fees "reasonably calculated to reimburse it for its actual cost in making such records available." It further permits local government to include in its fees "costs for summarizing, compiling or tailoring a record to meet the person's request." "Actual cost" may include a charge for the time spent by staff to locate the requested records, review the records to delete exempt material, supervise a person's inspection of the original documents in order to protect the records, copy records, certify documents as true copies or send records by special methods such as express

mail. It can also include the cost of an attorney reviewing and segregating records that should not be disclosed.

4. **How long do I need to keep my e-mail?**
   Since e-mail is a method or a tool for communicating, a blanket retention for "E-mail Records" does not exist. Therefore each message needs to be evaluated for content to determine which retention to apply. The State Archives works with state and local government agencies to determine the proper amount of time (i.e. 3 years) a particular record needs to be kept. These "retention schedules" are your legal authority to dispose of public records and can be obtained through your City Recorder, County Clerk, agency records officer or by contacting the State Archives.

5. **Are messages sent from the office using a free or private e-mail account public records?**
   Work done on private e-mail accounts as well as personally purchased computers and hand held devices might be considered a public record for both access and retention/disposition, if the work meets the requirements of a public record defined in ORS 192.

6. **It is acceptable for Councilors to discuss City business using their personal e-mail systems without concern for open meeting laws?**
   No. In our quest for efficiency, we use computers to communicate with each other and with our constituents. This kind of communication may put us at risk of violating Oregon's open government laws, specifically the public records and open meeting laws. These laws were adopted to ensure that the government process remains open to the public. Oregon's Public Meetings Law applies to all government entities in Oregon and defines a meeting as the convening of an Oregon government entity "for which a quorum is required in order to make a decision or to deliberate toward a decision on any matter." (ORS 192.610(5)) The requirements for a quorum can be met at a local government meeting (i.e. City Council meeting) or in any electronic forum. All records of conversations or discussions of the quorum, including paper records, e-mail messages, or transcripts of on-line chats, are considered public records for the purposes of access and retention.

Sources

League of Oregon Cities, LOCal Focus, September 2002
OAMR Records Management Manual
"Oregon Attorney General's Public Records and Meetings Manual"
Secretary of State Archives Division
<http://arcweb.sos.state.or.us/recmgmt/e-mailfaq.html>
E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication, Nancy Flynn and Randolph Kahn, AMACOM (NY, NY) 2003.
The E-Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies, Nancy Flynn, AMACOM (NY, NY) 2000.

Chapter 2
Writing a Policy

Introduction

Sending, receiving, and creating documents and information electronically have become the norm in the business world. A record can take many forms, such as electronic data, microfilm, or paper. A written e-mail policy that addresses access, use and retention of e-mail will establish the rights and responsibilities of the employees using the system and help to reduce the risks associated with e-mail.

Purpose

This chapter will help you to develop an effective e-mail policy that addresses the use and access of the e-mail system and the retention of messages sent and received by the system. The chapter will also present ideas on training employees as to the proper uses of e-mail and offer tips on how you can measure the effectiveness of your policy. A strong written policy is the best defense your agency has against e-mail abuses.

Types of E-mail Messages and when it is a Public Record

E-mail messages come in many forms. Some messages are clearly business related while others are of a personal nature and still others come as unsolicited advertisements (spam). Other messages are meant to inform and no reply is needed (temporary or transitory messages) and finally we have those messages that are meant to solicit a reply. Below are examples of the various types of e-mail messages:

- **Personal e-mail** can be defined as a personal exchange not covered by the State of Oregon records retention schedule. This type of e-mail should be extremely limited in use and deleted after it is read.

Example:

To: Chris
From: Sue
Subject: Dinner

Chris, I'll pick up dinner tonight.
See ya at 7 p.m.!
Sue

Other examples of personal e-mails include:

- Lunch plans
- Jokes
- Chain letters
- Messages to family and friends
- Attached files such as photographs

Note: Minimize your use of your agency's e-mail system for personal purposes. Remember, e-mail messages are subject to discovery under the Public Records Act.

¿ **Spam** is an unsolicited e-mail message usually containing some form of advertisement.

Example:

To: Mary
From: Market Access
Subject: Discount Pills

Get great deals on prescription drugs!

Other examples of spam include:

- ¿ Free Money
- ¿ Great deals on products and services

Note: Spam is very hard to control. You may want to consider spam filters for your e-mail system. Another way of controlling spam is not to open a message that appears to be spam or from an unknown source. By opening spam you verify that your address is real, subjecting you to more spam messages. Spam messages need to be deleted immediately.

- **Temporary or transitory e-mail messages** are any exchange of communication that is fulfilled almost immediately upon request. Keep these messages until the task is complete or their value has passed.

Example:

To: Mike
From: Fred

Mike, send me the e-mail when you get a chance. Fred

Other examples of e-mail with temporary / transitory value:

- Charity campaigns
- Listserv messages
- Company-wide communications
- Meeting reminders
- Deadline reminders
- Routing slips
- Fax confirmation
- Reading materials
- Reference materials
- FYI e-mail information does not elicit a response

Note: Unnecessary retention of temporary e-mails can drive up storage costs and damage organizations in litigation. Remember that your e-mail is never private.

- ¿ **E-mail messages soliciting a response** is any exchange of communication that requires the recipient to respond or to perform an action on the message received. These messages may include attachments that the recipient will also need to respond to. The retention of these e-mails and any accompanying attachments will depend upon the content of the message.

Example:

> To: Joe
> From: Sam
>
> Enclosed are my fourth quarter figures. Please add yours in the appropriate columns and return it to me ASAP!

Other examples of e-mails soliciting responses are:

- Contract negotiations
- Administrative of fiscal communications
- Policy drafts
- Reports
- Requests for information

Note: E-mail messages that require a response are almost always public records in relation to access and retention. Remember that the e-mail system is not a secure medium and information of a confidential or sensitive nature should **never** be sent via e-mail.

Writing Your Policy

An effective e-mail policy is one that addresses the use and access of an e-mail system, addresses retention of the e-mail messages, provides for the training of each employee on what the policy means and how it works, and finally, allows you to monitor the actions of the system your employees to determine the effectiveness of the policy.

When to use E-mail

Every good policy will address how and when e-mail should be used by the agency. It will define what is appropriate use, what types of messages should not be sent over the e-mail system and consequences if an employee violates the agency's written policy.

A good policy will state that e-mail should be used for work purposes but may allow for personal use during scheduled breaks and lunches. The policy should also define whether or not subscriptions to work related listservs are allowed; if privately owned personal digital assistants (PDA's) can be used to receive and send work related messages and how those messages will be transferred to the agency's e-mail system or network; if work related discussions can occur in chat rooms or from private e-mail accounts; and in the case of elected officials (i.e. city councilors, county commissioners, etc.) whether e-mail discussions about agency business between members of the council/commissioners constitutes a quorum, and therefore subject to the Oregon Public Meetings Law (see Chapter 1).

Below are some examples of good e-mail use statements. More examples can be found in the Appendix of this manual.

Example 1

"Appropriate Use. (a) E-mail shall be used for business matters directly related to the business activities of the [Agency] and as a means to further the agency mission by providing services that are efficient, complete, accurate, and timely. (b) E-mail shall not be used for personal gain, outside business activities political activity, fundraising, or charitable activity not sponsored by the State of Oregon or the [Agency]. (c) E-mail shall not be used to promote discrimination on the basis of race, color, national origin, age, marital status, sex,

political affiliation, religion, disability, or sexual preference; promote sexual harassment; or to promote personal, political or religious business or beliefs."

Example 2
"Electronic mail systems are intended to be used primarily for business purposes. Any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not potentially embarrass the [Agency]. All messages sent by electronic mail are [Agency] records."

Example 3
"The use of privately owned e-mail accounts or personal digital assistants (PDA's) for sending and receiving work related e-mail messages, may be used but is not recommended. However, if these resources are used for work related purposes, the user must transfer all work related messages to an agency owned system or network and must realize that these private accounts and PDA's may be subject to public disclosure and retention requirements. PDA's that are the property of the agency are subjected to the same use rules and expectations outlined in this agency's acceptable use policy for …"

Example 4
"Internal sensitive or confidential subjects (including our customers) should not be discussed via e-mails..."

You may also want to include in your policy on acceptable use, the expectations for content, style, and tone also commonly referred to as 'netiquette.' See Chapter 7 for more detail on e-mail etiquette.

Users must take the same care in drafting an e-mail message as they would for any other communication. Most e-mail systems are not secure. You should assume that people other than the recipient would be able to read your e-mail message. Confidential information should **never** be sent either in the body of an e-mail message or in an attachment.

Access to E-mail Accounts
An effective e-mail policy will clearly define and state who has access to individual e-mail accounts. If you plan on allowing supervisors and other employees in a position of management to monitor, access and review individual e-mail accounts then you need to clearly state this in your policy.

Below are some examples of good e-mail access statements. More examples can be found in the Appendix of this manual.

Example 1
"PRIVACY/PUBLIC ACCESS. (a) The [Agency] reserves the right to monitor e-mail messages and to access employee e-mail."

Example 2
"[Agency] reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose. Supervisors may review the electronic mail communications of workers they supervise to determine whether they have breached security, violated…policy, or taken unauthorized actions. [Agency] may also disclose electronic mail messages to law

enforcement officials without prior notice to the workers who may have sent or received such messages."

You may also want to address the use of an employee's e-mail account by another employee.

Example 1
"No employee shall read e-mail received by another employee when there is no business for doing so."

Example 2
"No employee shall send e-mail under another employee's name without authorization."

Example 3
"No employee shall change any portion of a previously sent e-mail message without authorization."

Retention of E-mail Messages
If an e-mail message is a public record then it is subject to retention requirements based on the content of the message. How you choose to retain these messages should be clearly stated in your e-mail policy.

Messages may be retained as part of the e-mail system or copied and filed in another more appropriate electronic filing system, printed and filed as part of a paper filing system and then deleted from the e-mail account, or by using a combination electronic/paper filing system. The retention of e-mail messages is discussed in more detail in Chapter 3 "Retention/Disposition/ Filing" of this manual.

The following is an example of a good e-mail retention statement. More examples can be found in the Appendix B of this manual.

Example 1
"…all E-mail communication other than those defined as non-record by ORS 192 shall be printed and filed in accordance with procedures established by each unit for maintenance of its files. Non-record communications may be deleted when read."

Policy Awareness
It is one thing to have a great written policy that covers all aspects of e-mail use, access, and retention and entirely another in making employees aware of the policy and what your expectations are for using e-mail. Every employee should be given his or her own copy of the agency's e-mail policy. At the end of the policy there should be a space for the employee to sign and date the policy, affirming that they have read the policy and understand the consequences for failure to comply. Be very clear in stating the consequences for failure to comply. Below is a good example of this:

Example 1
I have read the above policies and agree to comply with them. I further understand that non-compliance will result in appropriate disciplinary action, up to and including dismissal from state service.

Name of Employee (printed)	Date
Signature of Employee	Date

Signed policies must be returned to the supervisor and filed in a secure location. It is also strongly recommended that each employee receive training on your agency's e-mail policy. See the Appendix for an example of this training.

In addition it is important to create relevant points of contact within the policy so that lines of accountability are established if any questions or issues arise relating to the use, access, and retention of e-mail messages. Delineate what role the recorder, the IT staff and anyone else has relating to this policy and note who is to be contacted regarding specific issues that are discussed within the policy.

Training

Policies and procedures are useless if employees do not know how they apply to their daily activities at work. Training is a crucial part of policy awareness and compliance. Training activities need to be created that work with each agency's corporate culture, workload and schedules. Whether it is a web-based tutorial, a presentation from a trainer or giving each employee a specific amount of time to read the policy and ask questions, training is the key to an effective and well-referenced policy. An example of a training application can be found in the Appendix C.

Ensuring and Enforcing Policy Compliance

It is important to monitor how your agency is complying with your e-mail policy. This can be done in a number of ways, including surveying employees on their use of the system, sampling back-up tapes, and monitoring an employee's job performance.

If you suspect an employee is violating the agency's e-mail policy, you must act at once. Consistency in enforcing your policy is your best defense. The rules outlined in your policy must apply to all employees, regardless of their status and/or rank.

Chapter 2 - Case Study

Josey Bag O'Donuts, a partner in a consulting firm, has contracted with a large city to evaluate its e-mail use and retention policy. The City Manager has told Josey that there are numerous e-mail use and retention policy statements originating at all levels, from department heads, division managers and even the city council. Procedures for implementation do not accompany the policies. Josey has also contacted a number of individuals within the city to determine the type of e-mail use, access, and retention procedures currently in place. The conclusion is that there are no consistent, established policies or procedures for the use, access or retention of e-mail within the city. What

steps should Josey take to assess the problem and improve the city's e-mail use and retention policy? Is the city exposed to litigation by not having a written e-mail policy in place? Explain.

First, Josey should consult with all units that have issued policies to consider the strengths and weaknesses of the existing policies. Next, Josie may want to form a working group consisting of representatives of units that have policies and those that don't to formulate a single, city-wide policy and procedure. The group could begin by consolidating the strong parts of existing policies and strengthening weak parts and adding to the policy ensuring that the policy is comprehensive. She could also choose to do the above on her own, consulting with city employees as she develops the policy. Once the policy is written and approved for use by the city, Josie should work with the city to develop detailed procedures for implementation and training. Additional policies relating to employee compliance should also be addressed by Josie.

Second, the absence of written policies and procedures for e-mail is a liability for the city. Without written policies and procedures, there is little to no consistency in using the e-mail system, uncertainty as to access to the messages within the system and no clearly define rules as to what messages need to be retained and how employees should retain them. The lack of written policies and procedures may appear suspicious in the event of litigation or audit. The best defense against litigation and audit is a written policy, signed by each employee stating that they understand the contents of the policy, frequent employee training on the policy, and a mechanism in place to monitor compliance to the policy.

Chapter 2 - Quiz

True or False

1. **Public employees do not need to follow the General Records Retention Schedules when it comes to their e-mail messages?**
   False. If an e-mail message is a public record (see Chapter 1) then the message is subjected to the retention periods found in the General Records Retention Schedules OAR Chapter 166 Division 200 (cities) and OAR Chapter 166 Division 150 (counties and special districts).

2. **All e-mail messages are covered under the State of Oregon Records Retention Schedule.**
   False. E-mail messages that are not public records (see Chapter 1) are not listed in the general schedules and do not need to be retained.

3. **The most inexpensive way to store e-mail is on my computer.**
   False. Depending on the e-mail system, storing messages electronically may be more expensive than printing and deleting, especially if the system does not allow for messages to be deleted once they are stored. You will also want to consider the security of the system. If the system is not secure, your agency may be assuming additional risks and liabilities.

4. **My personal PDA, which includes my work calendar, is not subject to discovery.**
   False. If you use your PDA to perform public business or if you create, receive, send or file and record public records (see Chapter 1) then your PDA will be subject to discovery.

5. **Every e-mail message that I receive should be opened and read.**
   False. E-mail messages from unknown or suspicious addresses should not be opened in case they contain viruses. In addition, obvious spam messages should not be opened, because this verifies that your address is active and could subject you to additional spam messages.

6. **E-mail is not considered a record since it is intangible.**
   False. E-mail may be a public record. See Chapter 1 for more information on the definition of a public record.

Sources

NARA Records management ERM Overview. www.archives.gov/records_management
E-mail-policy.com www.e-mail-policy.com
MessageRite – Free E-mail Policy Template www.messagerite.com
E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication, Nancy Flynn and Randolph Kahn, AMACOM (NY, NY) 2003.
The E-Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies, Nancy Flynn, AMACOM (NY, NY) 2000.

Chapter 3
Retention / Disposition / Filing

Purpose
This chapter will help you to identify those e-mail messages that are subjected to retention and disposition requirements, provide you with three options for retaining messages until their retention requirements have been met and assist in establishing a simple filing system for your e-mail messages.

Identifying E-mail Messages Subjected to Retention
Many e-mail messages fall under the definition of public record found in Oregon Revised Statutes (ORS) 192.005 (5). E-mail that constitutes a public record needs to be identified, managed, protected and retained for as long as needed to meet the administrative, legal, financial, and historical needs of the agency.

Records needed to support program functions should be retained, managed and made accessible in a separate filing system in accordance with the appropriate program unit's standard filing practices. Users should:

Delete e-mail records after they have been filed in a record keeping system
Delete records of transitory or little value that do not document agency activity

Examples of messages sent by e-mail that typically are public records include:

Policies and directives
Correspondence or memoranda related to official business
Work schedules and assignments
Agendas and minutes of meetings
Drafts of documents that are circulated for comment or approval
Any document that initiates, authorizes, or completes a business transaction
Final reports or recommendations

Examples of messages that typically do not constitute a public record are:

Personal messages or announcements
Copies or extracts of documents distributed for convenience or reference
Announcements of social events
Messages received via a listserv
Spam

As with other records, retention periods for e-mail records are based on their administrative, legal, fiscal, and historical value. E-mail itself is not considered a record series. E-mail is simply a medium that creates and transmits records that have retention periods. Public business is subjected to the same laws, regardless of whether it is in a paper filing system or an e-mail system. Before you can identify the retention period of an e-mail message, you must examine its content. You can then determine what type of record the e-mail actually is and which records series it should be filed with.

In other words, each e-mail message must be categorized and classified according to its content, rather than simply lumped in with all other e-mail messages. E-mail should be retained in accordance with written retention policy and rules (see Chapter 2--Writing a Policy). Following these retention rules will protect both employees and the organization.

The same rules that apply to paper records also apply to e-mail messages in that only one copy, the "official" or "record" copy, of the message needs to be kept when multiple copies exist. (OAR 166-005-0010 (7))**.** *Extra copies of a document, preserved only for convenience of reference, require no prior authorization for destruction (ORS 192.005(5)(d)).*

Because an e-mail message may be filed in multiple records series, users should identify any and all records series it belongs to. An e-mail message will generally have the same retention period as records in other formats that are related to the same program or function. For example, e-mail relating to an agency's budget submission would be handled and retained just as any other budget record.

Many e-mail messages are easily recognized as program records and will be filed with the relevant records. Other e-mail messages may be correspondence related to the program record. These messages will also be filed with the relevant records and have the same retention period (i.e. the budget record example from above). Correspondence has been defined as:

Correspondence
Records that:
1. document communications created or received by an agency AND
2. directly relate to an agency program or agency administration AND
3. are not otherwise specified in the City General Records Retention Schedule (OAR 166-200), County and Special District General Records Retention Schedule (OAR 166-150) or in any agency special schedule or in ORS 192.170.

Records may include but are not limited to letters, memoranda, notes and electronic messages that communicate formal approvals, directions for action, and information about contracts, purchases, grants, personnel and particular projects or programs.

Disposition: File with the associated program or administrative records. Retentions for records can be found in the City General Records Retention Schedule (OAR 166-200) or the County and Special District General Records Retention Schedule (OAR 166-150). Communications not meeting the above criteria do not need to be filed and may be retained as needed.)

Just as with e-mail messages, attachments can belong to any records series. The attachment should always be filed together with the complete e-mail message, along with all header information and message text.

Methods for Preserving E-mail
Unless your e-mail system has been set up to handle retention and disposition, e-mail messages should not be retained in e-mail systems for extended periods of time, but should be filed in a separate system and deleted from the e-mail system in a timely fashion. To retain information in an

e-mail message for an extended period, it should be either transferred from the e-mail system to an appropriate electronic system or printed and filed in an existing paper filing system.

There are three basic methods of preservation for e-mail: electronic, paper and a combination of the two. Regardless of the method you choose, your priority should be to ensure that you keep only e-mail messages whose retention periods have not been met and that all others are deleted. Deciding which technique to use may hinge on such issues as cost, your office's access needs, and the technical capability of your staff.

Electronic filing system - The first option discussed here is retaining e-mail messages electronically. Your e-mail system may already be set up to store and retain messages for a limited period of time, or your system may be set up to transfer the messages from the e-mail system to some other type of electronic storage system. Still other methods of electronic filing systems require the user to convert the message to a text file and then to store that text file in another system. Whatever the electronic system may be, you need to be aware of the limitations of this type of filing system. These limitations may include:

- Hardware and software obsolescence--for example, if your e-mail software company goes out of business or is bought by a competitor, your e-mail system may not be supported. This will require your organization either to migrate e-mails periodically from one e-mail format to another, or to save the e-mail message in a standard format.
- Conversions to text files can be labor-intensive.
- A migration plan would need to be developed to make sure messages are accessible until the retention period has been met.
- Preserving metadata (data that describes data).
- Deletion of messages once the retention period has been met.

Paper filing systems - The second option is to print e-mail messages and interfile them with paper records. If you choose paper as a preservation medium, remember that printing e-mail for retention purposes is acceptable if you print the message and any attachments with all header information (metadata) intact; i.e., time and date, routing info, etc. This option is inexpensive, eliminates duplicate filing systems, and frees up space on servers and hard drives. The limitations of this option include:

- Messages are no longer searchable.
- Metadata and digital signatures may be lost.
- E-mail records may be inadmissible in court if they are not printed out with all their metadata.
- Printing messages is time-consuming and may be labor intensive.

Combination of both electronic and paper filing systems - Using a combination of the above may be beneficial for your agency. With this system, you may choose to retain messages with shorter retention periods electronically, while messages with longer retention periods are printed and filed. Limitations are similar to the above and may also include:

- Confusion as to what needs to be retained in which format.
- Loss of information.

Whichever method you choose, be sure to clearly define it in your e-mail policies and procedures (see Chapter 2--Writing a Policy).

Note: It is important to remember that saving records to your hard drive is not a viable preservation strategy since all of your work can be wiped out in the event of virus, exposure to moisture or temperature extremes or disk defect. In addition, security back-ups do not constitute a long-term storage plan. Back-up tapes serve as a security copy in the event of disaster or large data loss and do not provide a way to search records or to maintain complex links between records. Long-term storage takes into consideration records retention and scheduling, and creates an environment for easier retrieval. Back-ups are not a substitute for the long-term storage of records on reliable storage media.

E-mail Retention – General Comments

Management of e-mail messages in accordance with retention schedules is necessary to comply with federal and state law. A strong records management program is the surest way to preserve only those records required by law and to dispose of the rest when their retention periods have expired. In determining which e-mail messages should be retained or deleted, you should first consult your agency's records retention schedule. An informed e-mail management procedure that complies with the law requires a trained and knowledgeable workforce. This is also the best defense against lawsuits. Therefore, training employees on the classification, retention and disposition of electronic messages should be an ongoing process.

Records retention can be a time-consuming process and retention of e-mail records can be particularly problematic. Individual users are often responsible for managing their own documents in the system, which can lead to dispersal of similar records and inconsistencies in the amount of time that records are retained. Each agency must develop its own system to manage retention and disposition and inform staff of that system through policies, procedures, training, and education. It is particularly important for the agency to develop uniform practices for maintaining e-mail messages that are records, and ensuring their continued accessibility as an agency resource.

E-mail Disposition

Disposition refers to the final phase of a record's life cycle. This means either destruction of a record that is no longer needed or permanent retention of a record that has been determined to have historical value to your agency. Pursuant to the policies and procedures of each agency, an e-mail message may be deleted once its retention period is reached**.**

Policies and procedures are crucial to establishing a routine for disposition. While destruction of records on a regular basis is viewed as an acceptable business procedure to increase efficiency, hurried bulk destruction of records can be viewed as suspicious, particularly if an audit or lawsuit is imminent. State law prohibits the destruction of e-mail or any other public record not listed on a current retention schedule. The law also prohibits the destruction of records before their retention period has been reached. Records destruction request forms that have been signed by records managers and agency policies pertaining thereto, will provide legal protection in the event that a record is subpoenaed after it is destroyed.

With planning, policy and training, your agency can comply with the laws regarding retention and disposition of e-mail records. Your agency's records retention schedules should be consulted before disposing of any records, whether in paper, microfilm or electronic form. The Archives Division is available to answer any questions not addressed by this manual.

Organization and Filing

Filing practices for e-mail are not unlike filing practices for other office correspondence. Like paper records, many e-mail messages are easily associated with an entry in a records retention schedule and for e-mails messages that could reasonably go into several categories, you may want to add a cross-reference to the other filing locations.

One acceptable option is to retain e-mail messages in an electronic environment outside of the e-mail system that created it. Be as clear as possible regarding who is responsible for filing. This may be done as part of your written policies and procedures. You may also choose to add a disclaimer at the bottom of every e-mail declaring the recipient and sender's responsibilities in filing the message. However, you need to keep in mind that enforcement of disclaimers can be very difficult.

Filing Systems

Considerations for filing include ease of use for all users, as well as costs. If e-mail messages will be organized and filed electronically, you will want to consider not only costs for personnel, but also costs for hardware, software, technical support and electronic storage.

Filing practices for e-mail messages are comparable to filing practices for other office records. The recommended method is to use the same filing scheme for paper and electronic files. You can set up as many folders as you need to organize your records in a way that makes sense to you. One recommendation is to set up folders by record series and retention or by project. If you have a file on your desk titled "Purchasing Records, 2003," you may want to assign the same folder title to your electronic materials on that subject. Remember, filing systems should be simple, logical and easy to implement; otherwise, they will not be effectively used.

Summary

The goal of any program for managing e-mail messages should be to integrate the e-mail message into a total management program, one that covers all records – paper, electronic and otherwise. E-mail users require guidance on which e-mail messages can be deleted, which must be filed and how to dispose of e-mail messages once their retention period is reached.

Chapter 3 - Case Study

A business owner, John Davis, e-mails the city requesting a business license. The city responds that license applications are not yet accepted by e-mail and must be submitted in person at City Hall. One year later, when Mr. Davis is charged with operating without a business license. He files suit against the city, alleging that his attempts to obtain a business license were ignored. How do you go about defending against the lawsuit? How would your office locate records that would disprove the allegations?

If properly managed, e-mail can help the city defend against lawsuits. A written city policy, distributed to employees and enforced by supervisors, should establish how e-mail messages are to be retained. This will simplify the retention and retrieval of messages in the event of Public Records requests or legal discovery.

The city should have treated the e-mail message as a business communication and physically retained it according to city policy for the entire length of the retention established in the City General Records Retention Schedule. If both messages have been retained, it will be quickly established that the city did respond in a timely manner and instructed Mr. Davis in the proper way of obtaining a business license from the city. However, if no policy existed on retaining e-mail messages and city staff could no longer produce the messages relating to this transaction, then the city may be held liable. The IT department's maintenance of an e-mail system's backup tapes is not a sufficient means of retaining records. While IT policies vary across government, many agencies reuse backup tapes on a regular basis. By comparison, retention schedules can require certain e-mail messages to be kept for long periods of time such as 30 years or even permanently.

Other issues to consider:
Can the city produce a written procedure relating to business license applications and demonstrate that the procedure was followed in this case?

Did the city's policy and procedures for e-mail specify how the e-mail message was to be kept--electronic, paper or a combination of the two? If the policy required e-mail messages to be printed, deleted from the system and filed, were the proper metadata tags (message headers, etc.) saved in addition to the message text?

Chapter 3 - Quiz

1. **Can messages in an e-mail system be relevant to city/county/special district business?**
   Yes. Many e-mail messages directly relate to an agency's business. Public business is subjected to the same laws, regardless of whether it is in a paper filing system or an e-mail system. See Chapter 1 Public Records Issues

2. **When can I delete e-mail messages?**
   a. **Immediately**
   b. **When I no longer need them to do my job**
   c. **It depends on the retention period associated with the record**

   The correct answer is C. Before you can identify the retention period of an e-mail message, you must examine its content. You can then determine what type of record the e-mail actually is and which records series it should be filed with. In other words, each e-mail message must be categorized and classified according to its content, rather than simply lumped in with all other e-mail messages. E-mail should be retained in accordance with written retention policy and rules (see Chapter 2--Writing a Policy). Following these retention rules will protect both employees and the organization.

3. **Your agency policy is to print and file each e-mail message that must be retained for administrative purposes. The e-mail message is then deleted from the e-mail system. The message text, or body, must be printed out. To provide context for the message and**

make it legally admissible evidence, certain information must also be included in the printout. This information is called:

a. content
b. metadata (data that describes data)
c. preservation

The correct answer is B. Metadata is data that describes data and in relation to an e-mail message includes data elements such as who the message is to, who sent it, time and date sent, and routing info.

4. **A public employee receives and sends e-mail messages on a variety of topics to recipients both inside and outside the organization. Is it acceptable to treat all this e-mail as one record series and to manage and retain it as a group for a uniform length of time?**
   No. Before you can identify the retention period of an e-mail message, you must examine its content. You can then determine what type of record the e-mail message actually is and which records series it should be filed with. In other words, each e-mail message must be categorized and classified according to its content, rather than simply lumped in with all other e-mail messages. E-mail should be retained in accordance with written retention policy and rules (see Chapter 2--Writing a Policy). Following these retention rules will protect both employees and the organization.

5. **A business document is e-mailed as an attachment. The business document is also filed in the office as paper records. Are the e-mail message and attachment subject to the same records retention schedule as the paper records?**
   *The records retention schedule only applies to the "Official" or "Record" copy of the information . ["Record copy" means the official copy of a public record when multiple copies exist. (OAR 166-005-0010 (7))**.** Extra copies of a document, preserved only for convenience of reference, require no prior authorization for destruction (ORS 192.005(5)(d)]. Once you have determined which version is the official copy, then that version will carry the retention requirements, regardless of its medium (electronic or paper).*

Sources

E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication, Nancy Flynn and Randolph Kahn, AMACOM (NY, NY) 2003.
The E-Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies, Nancy Flynn, AMACOM (NY, NY) 2000

Chapter 4
Security

Purpose
The purpose of this chapter is to introduce the issues and suggest steps or measures that might be taken by an organization to prevent unauthorized exposure, loss or corruption of vital information.

Introduction
An organization's strength in sharing information electronically may become a vulnerability if security is breached. This chapter explores those valued organizational characteristics that may be vulnerable to loss or corruption and offers suggestions for controls an organization might consider putting in place. Any controls put in place should not only address networked personal computers (PC) and servers but also stand-alone personal computers with dial-up modems. In addition to employees working from home, there may be contractors and consultants accessing the computer network.

Vulnerabilities
Information is one of our greatest assets. Local governments are responsible for preserving the public record and as much care should be given our electronic records as are given other media we carefully store under lock and key. Local governments are accountable for protecting records from unauthorized access, guarding confidentiality and preventing modification, destruction, theft and general misuse of information. Every organization should be able to confidently answer the following information security questions:

Confidentiality - Is your agency's information accessible to only authorized users?
Integrity - Is the accuracy and completeness of your agency's information and processing methods safe?
Availability - Is information available to authorized users so they can carry out their job duties?

Types of Controls
There are many types of controls an agency can implement. One relatively inexpensive method is the implementation of a user policy that serves the dual purpose of establishing rules and raising employee awareness. If funds are available, your agency may choose a less discretionary route and purchase security or encryption software for its network.

Usage Policy
Here are several suggestions you may wish to include in an administrative policy:

Lines of Authority

In order to effectively monitor the network and e-mail activity, certain lines of authority and responsibility should be established. Clearly define the roles of the system administrator and IT department, department managers and individual users. The person or group responsible for

network maintenance must establish the security policies and standards, ensure compliance and provide support and periodic training to managers and users. Managers must ensure employees under their supervision adhere to the established policies and standards and initiate disciplinary action when necessary. Users must understand and agree in writing, to comply with agency policies and standards.

User Privileges

Assign privileges based on what the user needs to perform his/her job to reduce the risk of lost or corrupted data. A user unfamiliar with proper procedures can do as much damage as someone with malicious intentions. Administrative privileges to all network applications should be granted on an extremely limited basis.

User Passwords

Passwords should not be shared with other users, although a department may wish to set up a confidential system of keeping managers informed of current passwords in the event a user is unexpectedly absent. To further protect the network, encourage users to avoid passwords that are family members' names, the favorite pet's name or a dictionary word. These types of passwords can easily be guessed.

Unattended Workstations

Encourage users to lock their workstations when they are absent for short periods of time to prevent an unauthorized person from browsing through files, sending messages or entering unacceptable Internet sites. Users leaving the building or who are for some reason unavailable for a period of time should be encouraged to shut down their computers. IT staff occasionally needs to take the network down or perform some service on a PC and cannot do so if the workstation is locked and the user is not available. Each agency should encourage the use of privacy screens by users handling confidential data.

Monitoring and the Expectation of Privacy

To ensure network integrity, authorized personnel may from time-to-time monitor user e-mail and Internet activities. Let users know that activity on the agency's network is not private, regardless of whether it takes place during regular work hours or remotely from a dial-up connection.

Message Opening and Forwarding

It is important to caution users not to open and/or forward e-mail from unknown senders. The 1999 Melissa Virus was devastating to Microsoft Outlook users. Once the e-mail was opened, the virus mailed copies of itself to the first 50 names in that person's address book. The virus was received from someone you knew and trusted. The 2000 ILOVEYOU virus was simply an e-mail attachment. The virus was launched when the recipient double-clicked on the attachment. Remind users to take some simple precautions and not let curiosity take over. These viruses cannot replicate without human help. Either delete a questionable e-mail or call IT Support. If you think you have inadvertently sent a virus to people in your address book, call and notify them.

Software Downloads

Agencies should issue policies prohibiting users from downloading any software from the Internet or other unknown source. Requests for necessary software should be directed to IT Support.

Sending Confidential Information

Establish rules relating to the type of information sent via e-mail. Do not transmit confidential or personal information such as credit card numbers and passwords unless the recipient has the proper safeguards in place.

Unwanted E-mail or Spam

Spam has increased to the point that it consumes over 50% of all e-mail traffic on the Internet. Rather than hitting the "delete" key a dozen times, investigate the options available for sending unsolicited e-mail directly to a trashcan for automatic deletion. IT Support can provide information on junk mail filtering software. Do not open obvious junk mail and do not attempt to remove yourself from the mailing list by replying. Any kind of response can verify to the sender that that your e-mail address is valid. Users are better off deleting unwanted e-mail immediately.

Contractors and Consultants

Discuss with your agency's legal counsel, the feasibility of adding language to your contracts and personal service agreements that address how contractors and consultants handle your organization's information and what the agency expects in terms of protection.

Reporting Security Concerns

Establish a clear process for reporting suspected security breaches including compromised passwords. Unusual behavior may be caused by a virus. Symptoms may include missing files, crashes, or misrouted messages.

Back-ups

Most IT departments have a data backup program in place. The loss of data can be inconvenient, but proper backups can help to restore what was lost.

Good Use of Resources

Discourage users from sending out virus alerts – leave this to the IT department. Unnecessary mass mailings should also be discouraged because they use up company resources and employee time.

Virus Protection Software

There are dozens of virus protection software products on the market to choose from as well as fixes provided by the software provider. Microsoft, for example, is a major target for hackers and regularly sends out patches for the program holes. It is important to keep up to date with all the new versions to adequately protect your PC and the network.

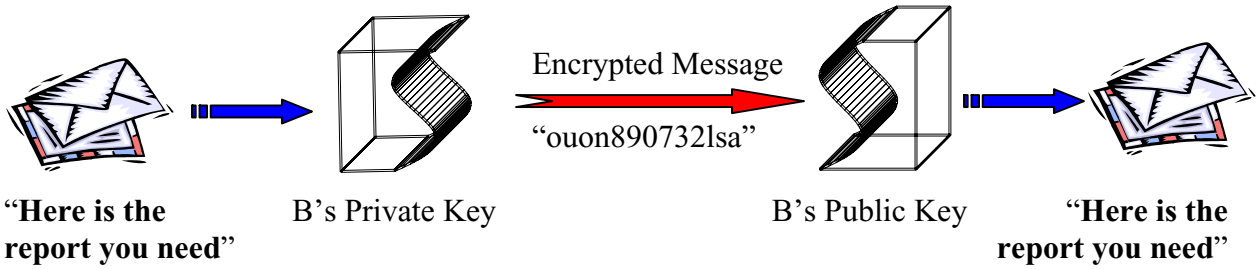
Encryption

When an e-mail is sent, it passes through numerous servers en route to its destination. Because most e-mail has no built-in security features, confidentiality and authenticity issues can arise. Encrypting

e-mail messages usually employs Public Key Infrastructure (PKI). Encrypting a message renders it undecipherable by others unless they possess the tool that decrypts the message. PKI issues all users within a system or community a private key, which is confidential and a public key, which is publicly held in a sort of digital signature "white pages". When encrypted with either signature, only your corresponding signature will decrypt the message. Digital signatures can be used to do two things (both of these encryption methods can be used on the same message to protect confidentiality and to ensure that the sender is who they say they are):

1) If sender A encrypts a message with their private key, recipient B can then decrypt the message with the sender A's public key. This method verifies that sender A really sent the message.

2) If sender A encrypts a message with recipient B's public key, recipient B can decrypt the message with it's own private key. This method secures the confidentiality of the message as its being sent so that no one can intercept it without the recipient knowing.



More effort will be required to secure a web server if an organization is accepting online payments, or receiving sensitive information such as a Social Security Number. In this case, information passes through an intermediary known as a certificate authority that both the sending and receiving computers "trust". It provides the asymmetric (public) key to each once the identity of each is verified.

Digital Signatures

Digital signatures ensure the authenticity of an electronic record, including e-mail, text file, etc. The transmitting computer sends the coded record in such a way that the receiving computer can verify the record is coming from a trusted source and that the record has not been altered in any way.

Firewalls
A firewall is a program or hardware device that filters information coming into a network at each Internet connection. At this point, an organization can put rules in place that flag certain incoming information and protect the integrity of the network as well as control user connections to the Internet. Without a firewall, hackers could take advantage of any security hole in the system. Firewalls use one or more of three methods below to control the information flow:

1. Packet filtering compares small chunks (or packets) of data against the filters or rules. Packets that do not make it through the filter are discarded.
2. Proxy service might be compared to a two-way messenger service that carries information between the Internet and the organization.
3. Stateful inspection compares key parts of a packet to a database of information. The firewall gathers defining characteristics of information going out from the organization, and incoming information is compared to these characteristics. If there is a reasonable match, the incoming information gets through the firewall. If the match is below standards, the packet is discarded.

Similar to a biological virus, a computer virus begins with the infection of one individual, spreads quickly and results in some very sick networks. If your organization has been lucky enough not to fall victim to hackers, you have certainly heard about many that have. Firewalls can filter out such things as:

- Application backdoors that are either intentionally built into a program to allow remote access or bugs that allow hidden access
- Denial of service attacks that crash servers and websites
- E-mail bombs that bombard the recipient with messages until the computer crashes
- Macros, originally designed to simplify complicated procedures, that hackers create to destroy data or crash a system
- Operating system bugs that allow backdoor access
- Redirect bombs that enable hackers using Internet Control Message Protocol (ICMP) to redirect the information path potentially resulting in a denial of service
- Remote login that allows an unauthorized user to access files or run programs
- Simple Mail Transfer Protocol (SMTP) hijacking that accesses e-mail addresses and sends thousands of unsolicited e-mails – "spasm" – to users
- Source routing that hackers employ to disguise a packet of information to look like it is coming from trusted source
- Spam, or unsolicited e-mail, can contain viruses and other malicious code

It is important to remember that while a firewall will increase a network's general security, it is also likely to mistakenly block some legitimate messages.

Chapter 4 – Case Study
Employee Bob Smith received an e-mail message from an address that he did not recognize. Because the subject of the message was "Business Opportunities" Bob opened the message. Shortly afterward, his computer crashed. He then noticed that his machine was acting sluggish and crashed

more than usual. Pop-up ads and offensive images filled his screen. Bob figured that it was just his computer acting up. By the time Bob recognized that something was seriously wrong with his computer, the virus had e-mailed copies of itself to many of his co-workers, crippling the network. What steps would you take to prevent this from happening to you?

The surest way to prevent infection is to never open or forward e-mail messages from unknown senders and to remember that viruses can disguise themselves as being from a friend or family member. In addition, never open an e-mail attachment unless you know who the sender is ***and*** *are expecting an attachment from them.*

In this case, with so many unrelated problems springing up, Bob should have assumed that the e-mail message contained a virus and notified the IT team at the first sign of computer trouble. His IT team should be able to troubleshoot the problem and tell Bob if all computers on the network are running antivirus software and receive regular virus definition updates, which reduce the likelihood of infection.

Computers can be unstable and it can be difficult for the average user to diagnose the cause of a computer problem. Users of your agency's e-mail system should be made aware of the ease at which viruses are transmitted through the e-mail system and the steps that need to be taken to minimize the risk of e-mail viruses.

Chapter 4 - Quiz

1. **What are three reasons an organization should consider additional security procedures?**
   The three reasons are to ensure the confidentiality of your agency's information accessible to only authorized users; to ensure the integrity (*the accuracy and completeness) of your agency's information and processing methods; and to ensure the availability of agency information to authorized users so they can carry out their job duties.*

2. **Circle the types of controls that an organization can implement to address security concerns within e-mail communications.**
   a. Lines of authority
   b. Passwords
   c. Spam filters
   d. Firewalls

   All should be circled. There are a number of measures mentioned in this chapter that will help your agency address security concerns. Some are very simple, such as not sharing passwords and some are more complex such as purchasing and implementing the use of encryption software. Decide which will work best for your agency and fit into its budget.

3. **What are some security risks that firewalls can alleviate?**
   Firewalls can help eliminate application backdoors that are either intentionally built into a program to allow remote access or bugs that allow hidden access; s*ervice attacks that crash servers and websites; e-mail bombs that bombard the recipient with messages until the computer crashes; macros that hackers create to destroy data or crash a system; operating system bugs that allow backdoor access; remote logins that allow unauthorized users to access files or run programs; source routing that hackers employ to disguise a packet of information to look like it is coming from trusted source; spam, or unsolicited e-mail, can contain viruses and other malicious code; and Simple Mail Transfer Protocol (SMTP) hijacking that accesses e-mail*

addresses and sends thousands of unsolicited e-mails – "spasm" – to users. In addition, fire walls can redirect bombs that enable hackers using Internet Control Message Protocol (ICMP) to redirect the information path potentially resulting in a denial of service

It is important to remember that while a firewall will increase a network's general security, it is also likely to mistakenly block some legitimate messages.

4. **True or False: Public employees have no expectation of privacy when it relates to monitoring employee e-mail usage on agency computer systems.**
   True. Public employees may have their e-mail usage as well as their computer usage monitored from time-to-time, by authorized personnel to ensure network integrity. Let users know that activity on the agency's network is not private, regardless of whether it takes place during regular work hours or remotely from a dial-up connection.

5. **You receive an e-mail from a co-worker, with an attachment and the subject line "THIS IS NOT A VIRUS!"**
   You should:
   a. Ask your co-worker if he/she sent you an e-mail
   b. Notify the IT staff that you received an unusual e-mail with "virus" in the subject line
   c. Assume that the e-mail contains a virus. Wait to open the message until IT staff advises that it is safe to do so
   d. All of the above

   The correct answer is D. Part of what makes a virus so effective is that it is deceptive. If a message looks suspicious then it probably is, so don't open it and notify your IT department at once.

Sources

E-Policy: How to Develop Computer, E-Mail, and Internet Guidelines to Protect Your Company and Its Assets, Michael R. Overly, AMACOM (NY, NY) 1999.
E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication, Nancy Flynn and Randolph Kahn, AMACOM (NY, NY) 2003.
The E-Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies, Nancy Flynn, AMACOM (NY, NY) 2000.
"Acceptable Use Policies, 'A framework for e-mail and Internet usage policies for your enterprise'" www.techrepublic.com
http://www.howstuffworks.com

- How do digital signatures work
- How firewalls work
- How computer viruses work
- How do viruses and worms spread through e-mail?
- How encryption works

"Electronic Mail Policy", University of California (2003) www.ucop.edu/ucophome/policies
"E-Mail Security", www.msexchange.org/articles/Email_security
"Vulnerability Management & the Security-Aware Organization by Visionael Corporation", Vendor White Paper (2003) www.knowledgestorm.com/search/viewabstract/61684

"Kansas Electronic Records Management Guidelines" – Kansas State Historical Society
www.kshs.org/government/records/electronic/electronicrecordsguidelines
"Electronic Records Management Handbook", State of California,
http://www.pd.dgs.ca.gov/recs/erm-toc.htm
"Virus Protection Guidelines", Financial Services Office, University of Arizona
http://www.fso.arizona.edu/fso/computing/Virus_policy.htm
"Information Technology Security Policy", South Dakota State University
http://www3.sdstate.edu/technologySupport/
"Establish a Bullet-Proof Security Policy", Ferrarini, Networking and Communications, article (2001) http://networking.earthweb.com/netsecur/article.php/897881
"Privacy and Security Policy", State of Texas Department of Information Resources
http://www.dir.state.tx.us/general_info/privacy.htm

Chapter 5
Technology

Introduction

We frequently integrate different forms of computer technology into our lives, even though we often lack a detailed knowledge of how it functions. We now rely on IT specialists when we have technical problems so that we can get our daily tasks accomplished on time. However, employees need to have a working knowledge of how their most frequently used technology functions. This chapter attempts to give an overview of several technological issues related to e-mail and other types of electronic messaging systems.

Purpose

This chapter presents reasons that agencies must stay current with technological developments in order to manage their e-mail systems. E-mail systems and storage software can require frequent upgrades. In addition, companies may refuse to support their outdated products. Most e-mail programs have certain system requirements and will work only with certain combinations of hardware and software. Internet-based technologies such as Instant Messaging can create serious records management concerns for your agency. With an eye to your agency's needs and budget, this chapter can assist you in selecting technology that will help meet your office's responsibilities to comply with records management statutes and the Public Records Law.

E-mail Storage Software

Your choice of technology will affect the efficiency of your office's communications, your ability to retrieve e-mail messages and your office's potential risk due to the retention and deletion of e-mail messages. Software applications can assist users by identifying and deleting junk mail, grouping and organizing e-mail messages and storing important e-mail messages for the long-term in a separate electronic system that meets the state's legal requirements. Software can also help users comply with records retention requirements:

- Managing incoming and outgoing e-mail messages, including deletion of email that no longer serves a business purpose and the transfer of important messages to a separate electronic system
- Surveillance and flagging of incoming and outgoing e-mail message content
- Security and audit trail capabilities
- Storage of messages and attachments on stable storage media

While the purchase of e-mail management software can be beneficial, agencies do not necessarily need to purchase one in order to organize and store e-mail messages. Most e-mail programs allow users to create and file e-mail messages in folders. Establishing folders that simplify filing (for example, by record series, retention period, or project) will help you place e-mail in the appropriate location and retrieve it at a later date. Folders or individual messages can be archived, which means that they are saved and managed at an alternate location (shared drive) or on backup removable media (CD-ROM, magnetic tape).

Integration of Messaging Technologies

E-mail can be sent and received on many types of devices:

1. E-mail-to-fax allows users to send faxes directly from their e-mail program, e-converted to a facsimile, arriving at the recipient's fax machine. Similarly, fax communications can be converted to a digital image and transmitted via the e-mail system.
2. Radio communication, such as a pocket paging system, allows short e-mail addresses to be sent to pagers. In more advanced applications, providers may lease notebook sized systems that can send and receive e-mail messages through earth-satellite relay.
3. Voice-mail systems accept e-mail messages for their clients. This is also known as "e-mail reading." The text in an e-mail message is funneled through a speech synthesizer to artificially read the e-mail message text into voice storage. Users can then listen to their e-mail messages by accessing their voice-mail system. E-mail reading can assist visually impaired users.

Storage and Preservation of E-mail Messages

As discussed in Chapter 3, there are numerous retention strategies for e-mail messages. Several examples are: maintaining the message in electronic form on a reliable storage media; printing out paper copies; and a strategy that employs both of the previous strategies. It is important to remember that saving records to your hard drive is <u>not</u> a viable preservation strategy since all of your work can be wiped out in the event of virus, exposure to moisture or temperature extremes or disk defect. Backing up data on a network creates an extra copy in case your hard drive is erased. However, this type of backup is not acceptable either, because in addition to the same vulnerabilities of local hard drives, other users can easily delete data. Chapter 3 discusses options in the section titled, "Methods for Preserving E-mail."

A distinction should be made between security back-ups and long-term storage. Security back-up procedures do not constitute a long-term storage plan. Back-up tapes serve as a security copy in the event of disaster or large data loss, and do not provide a way to search records or to maintain complex links between records. Long-term storage takes into consideration records retention and scheduling, and creates an environment for easier retrieval. Back-ups are not a substitute for the long-term storage of records on reliable storage media.

Technological obsolescence

Technological obsolescence refers to problems related to outdated hardware and software. Electronic documents can gradually become unusable over time without regular maintenance such as software upgrades and patches. They are vulnerable to technological obsolescence due to the ever-changing versions of software applications. This issue can arise with e-mail messages that are downloaded from one type of e-mail system and then the system is replaced by a different company's product. Files stored on removable storage media (i.e. cd-rom, tapes, dvd, etc.) are even more vulnerable and should be periodically "refreshed," or copied to new media.

Most common office software is proprietary, which means that it is owned and controlled by a company. When using proprietary software, users are at the mercy of the company that created it. Support for a product may be discontinued if the company goes out of business or merges with another company. This adds another challenge to the long-term storage and access to records created using that software.

Instant Messaging, PDAs, Chat Rooms and Alternative Communication Technologies
When deciding which types of software to make available for employee use, it is important to consider whether they will be used for public business and whether their adoption justifies the recordkeeping obligation that comes with them. In addition to e-mail systems, other Internet technologies have become very popular in communicating electronically. Communication via Instant Messaging (IM) and chat rooms happens instantaneously. Other types of communication technologies include: web-conferencing, project management and meeting software, weblogs (BLOGS), listservs, text messaging, and videoconferencing. If any of the above technologies are currently being used by your office to conduct public business, then the information being transmitted may be subject to the Oregon Public Records Law for both access and retention.
Just as with e-mail, policies need to be created for IM and chat rooms. This type of communication is difficult to retain due to its ephemeral nature and its web-based formats that are stored outside of your e-mail system. Oregon's Public Records Law requires the capture of all information that is considered a public record, which can include IM and chat rooms. Unless these conditions are met, these technologies may not be appropriate for agency use. (See Chapter 2 -- Writing a Policy and Appendix A -- E-mail and Instant Messaging Policy template).

Personal Digital Assistants (PDAs) are also becoming very common workplace accessories. Just like paper files in your office, e-mail messages and other electronic files on your PDA may have records retention and access requirements. E-mail messages, calendars, notes, task lists and the like need to be downloaded from the PDA to the appropriate locations on the agency's server on a regular basis. Your agency's records officer should be contacted for further information on which types of files stored on your PDA are considered to be public records.

There are many forms of technology available on the market. The key is to know your office's needs, resources and limitations to identify the one most suitable for your agency.

Chapter 5 - Case Study

You supervise a staff of three food inspectors who spend most of their time out of the office. To facilitate note taking, the three food inspectors purchased their own portable computers: one food inspector uses a laptop, the second uses a Blackberry, and the third uses a Palm Pilot. When they complete a project in the field, they circulate the information directly from their portable machines, sometimes using Instant Messaging (IM) software.

If a restaurant owner submitted a Public Records request for information on the handling of his case, how would you go about assembling the necessary records? How would you ensure that all the food inspectors' work product was also accessible from your office's network or e-mail system? How would you respond if a food inspector refused to comply with the request on the grounds that he owned the information on his machine because he had purchased it with his own money?

The agency needs to have a written policy that clearly states to all employees that their work on behalf of the agency results in the creation of public records, regardless of who purchased the equipment or their work location. In addition, the agency would need to have scheduled required data backups from all portable equipment to their network or e-mail system. If both of these were in place, the request would be a routine public records request. However, and let's assume since the employees are sharing information through Instant Messaging, the agency does not have any policies or data downloads. The agency would then have to take

each piece of equipment and try to reconstruct what took place. This action alone may compromise the integrity of the information. Without a means of tracking, storing, and retrieving public records communicated via Instant Messaging and chat rooms, their use should be expressly prohibited in a written policy.

If you decide that portable computer technology will enhance communication, customer service and efficiency, you should specify its legitimate work uses on one particular hardware and software product. This helps to keep the collected work product consistent, and simplifies its retrieval, storage and migration to newer formats in the future.

Chapter 5 - Quiz

1. **In what ways can e-mail management software help you to manage e-mail?**
   Software applications can assist users by identifying and deleting junk mail, grouping and organizing e-mail and storing important e-mail messages for the long-term in a separate electronic system that meets the state's legal requirements. Software can also help users comply with records retention requirements by managing incoming and outgoing e-mail messages, including deletion of email that no longer serves a business purpose and the transfer of important messages to a separate electronic system; surveillance and flagging of incoming and outgoing e-mail message content; by providing security and audit trail capabilities and storing messages and attachments on stable storage media

2. **What are some recent technologies available to e-mail users?**
   a. E-mail to fax
   b. Pocket Paging System
   c. Voice-mail systems that accept e-mail messages
   d. All of the above
   The correct answer is D. In addition other technologies such as PDA's and Blackberry's are available for use in a mobile setting.

3. **If a public employee sends e-mail message from a personal account on work time, could the e-mail be considered a public record?**
   Yes, if the message is related to public business.

4. **Is your computer hard drive a reliable media for long-term preservation of e-mail messages?**
   No. It is important to remember that saving records to your hard drive is <u>not</u> a viable preservation strategy since all of your work can be wiped out in the event of virus, exposure to moisture or temperature extremes or disk defect.

5. **Do Internet Chat Rooms, Instant Messaging, and other forms of electronic communication fall under Oregon's Public Records Law and Public Meetings Law?**
   They can. Remember, Oregon's Public Records Law does not discriminate based on the medium used to transfer public information. If you do public business via these means, you may be creating public records (See Chapter 1 for the definition of a public record).

Sources

http://www.webopedia.com/
E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication, Nancy Flynn and Randolph Kahn, AMACOM (NY, NY) 2003.
The E-Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies, Nancy Flynn, AMACOM (NY, NY) 2000.

Chapter 6
Budget

Introduction
All agencies are familiar with cost constraints and e-mail management comes with a unique set of costs. Agencies can reduce their postal service expenses by utilizing an e-mail system, but this savings may be offset by increased spending on computer equipment and in the management of the system's messages. It is important to keep in mind that vendor companies may require the purchase of annual software licenses or charge for technical support.

With proper planning, you will be able to prioritize your needs and decide what solutions you can afford. The key to a successful budget is planning. Many shy away from planning and see it as an unnecessary use of time and expenses, but the planning process helps to ensure the success of your project. Budgets for e-mail management projects will vary by the size of the government entity and the objectives you are hoping to achieve. The following checklists should give agencies a basic knowledge of the types of costs they will encounter.

Basic Costs
- **Staff Resources/Employee Time** - evaluating and selecting a solution, policy development, installation and implementation
- **Infrastructure/Equipment** - hardware, software, servers, telecommunications devices, temporary backup and long-term storage devices and removable storage media such as magnetic tape, CD-ROM, and microfilm
- **Maintenance and Upgrades** - for hardware and software systems
- **Security Resources** – firewalls and antivirus and spam-filtering software
- **Training** - in-house or external employee training on the e-mail system
- **Disaster Recovery Planning** - includes disaster preparedness and procedures to be followed in case of an emergency

Optional Costs
- **Records Management Software** - can automate filing, retention and deletion of messages
- **Customized Programming** - makes software more useful to your organization
- **External Consultants and Trainers** - can lend their experience and qualifications but the expense can be prohibitive
- **Off-site Storage** – for e-mail system back-ups

Ongoing Costs
- **Maintenance of Infrastructure/Equipment** - hardware, software and peripherals such as printers, scanners and servers
- **Hardware and Software Upgrades**
- **Data Migration –** moves existing information to newer software versions or to different software products
- **Training** - regularly scheduled employee training reviews on use of the system

Chapter 6 - Case Study

You are assigned to select a new e-mail system that complies with information security requirements and the requirements of access and retention under Oregon's Public Records Law. You are given a budget of $50,000 to complete the project. What steps do you take? Which item or items do you prioritize above the others? If, in your opinion, the budget is insufficient to accomplish your goals, how would you justify the appropriation of more funds to the project?

Although every office will have unique needs, the first step in every case should be planning. With proper planning, you will be able to prioritize your needs and decide what solutions you can afford. The key to a successful budget is planning. Many shy away from planning and see it as an unnecessary use of time and expenses, but the planning process helps to ensure the success of your project.

Some of these planning steps would include meeting with IT staff early in the process to notify them of your project and to solicit their input; developing requirements for use and access; developing requirements for the way your office will search and retrieve e-mail messages (text and headers) and developing requirements for managing and disposing of e-mail messages. These steps will help you to identify what items are a priority for the system, what can be purchased at a later time and what can be eliminated from the list. Priorities may include system size, back-up capabilities, networkability, basic security features, training and ease of use. Items to be purchased later may include additional storage, encryption software and an e-mail management system.

In justifying a larger project budget, you should emphasize that the potential costs of piecing together and trying to maintain multiple e-mail systems or the hidden costs of using an e-mail system that is insufficient, out of date or even obsolete. Stress your planning process and cost-benefit analysis that you have conducted as well as the agreed upon priority list.

Finally, when developing your budget, be sure to leave room for the ongoing costs since expenses don't end with the purchase of the equipment.

Chapter 6 - Quiz

True or False

1. **Planning for the purchase of a new e-mail system can be minimal since the vendors will explain what their product will do for you.**
   False. Although vendors are very versed in their product, they are not well-versed in your needs. Know what you want the system to do before you solicit vendors. Establish your budget and then a priority list what you need from the system now, what your ongoing costs will be, what you can purchase at a later date and finally, what you can live without. This will help to ensure that you get the product that will work best for you.

2. **The costs of an e-mail system end with its purchase.**
   False. There are many ongoing costs associated with any technology purchase. They include the maintenance of the infrastructure and the equipment - hardware, software and peripherals such as printers, scanners and servers; the need to periodically upgrade hardware and software (this may come as part of an annual licensing fee or may be a required extra purchase); migrating

data forward when new hardware and/or software is purchased and put into place and regularly scheduled employee training reviews on use of the system.

3. **Training is an item that you can eliminate when trying to cut costs.**
   False. Training employees on the proper use of the system will save the agency time and money because employees will know how to use the system efficiently which allows for better productivity. Instructing employees on the proper use of the e-mail system will also help to prevent misuse and abuse by employees and reduce potential agency liability in relation to e-mail use.

4. **Optional costs include records management systems and customized software.**
   True. Although both may be nice, they are not required to be used. Establishing a useful file plan/structure that allows users to file messages according to their content and project is basic and low cost. A well-established file structure can be converted at a later date to an electronic records management system. Customizing your software to your organization may be useful but the cost to do so may far outweigh its benefit.

5. **Regardless of size, all local governments will have to address the same items listed as "Basic Costs."**
   True. Regardless of size, each e-mail system will have to address the issues of staff resources/employee time, infrastructure/equipment, maintenance and upgrades of hardware and software systems, security resources, training and disaster recovery planning in order have an effective e-mail system. However, the size and scope of these issues may vary on agency size and complexity.

Sources

http://www.webopedia.com/
E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication, Nancy Flynn and Randolph Kahn, AMACOM (NY, NY) 2003.
The E-Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies, Nancy Flynn, AMACOM (NY, NY) 2000.

Chapter 7
E-mail etiquette

Introduction
The use of e-mail has become an important tool today for communicating as well as sharing and distributing information. As a communication tool, it is important to represent your agency in a professional manner, respond to e-mail clearly and efficiently and protect your agency from liability and unnecessary risk.

Purpose
The purpose of this chapter is to establish the expectations that your agency has for its employees when they are using agency e-mail systems. This chapter will provide email etiquette advice and rules to help employees become aware of their responsibilities when using the e-mail system.

Why do you need e-mail etiquette?
An agency should implement etiquette rules for the following reasons:

- Professionalism - by using proper e-mail language your agency will convey a professional image.
- Efficiency - e-mail messages that get to the point are much more effective than poorly worded e-mail messages.
- Protection from liability - employee awareness of e-mail risks may protect your agency from costly lawsuits.

What are the etiquette rules?
There are many etiquette guides and many different etiquette rules. Some rules will differ according to the nature of your agency and its corporate culture. Listed below are e-mail etiquette rules that could be applied to nearly all government entities.

E-mail cannot replace personal contact
There is a tendency to be less formal or careful when communicating using e-mail and that can sometimes provoke anger. Remember that direct, person-to-person contact is best for handling sensitive, difficult, complex or emotional issues.

E-mail is public
Assume the messages you send and receive are permanent and public. Don't say anything in an e-mail message that you would not want to be made public or forwarded to others.

Do not use e-mail to discuss confidential information
Sending an e-mail message is like sending a postcard. If you don't want your message to be displayed on a bulletin board, don't send it. Moreover, never make any libelous, sexist or racially discriminating comments in an e-mail message.

Use proper spelling, grammar and punctuation
This is not only important because improper spelling, grammar and punctuation give a bad impression of you and your agency, it is also important for conveying the message properly. E-mail messages with no full stops or commas are difficult to read and can sometimes even change the meaning of the text. If your program has a spell checking option, use it!

Read the e-mail message before you send it
A lot of people don't bother to read an e-mail message before they send it out, as can be seen from the many spelling and grammatical mistakes contained in them. Apart from this, reading your e-mail message through the eyes of the recipient will help you send a more effective message and avoid misunderstandings and inappropriate comments.

Use proper structure and layout
Since reading from a screen is more difficult than reading from paper, the structure and lay- out is very important for e-mail messages. Use short paragraphs and blank lines between each paragraph. When making points, number them or mark each point as separate to keep the overview.

Avoid long sentences
Try to keep your sentences to a maximum of 15-20 words. E-mail is meant to be a quick medium and requires a different kind of writing than letters. Also take care not to send e-mail messages that are too long. If a person receives an e-mail message that looks like a dissertation, chances are that they will not even attempt to read it.

Do not write in CAPITALS
IF YOU WRITE IN CAPITALS IT SEEMS AS IF YOU ARE SHOUTING. This can be highly annoying and might trigger an unwanted response in the form of a flame mail.

Be concise and to the point
Do not make an e-mail message longer than it needs to be. Remember that reading an e-mail message is harder than reading printed communications.

Don't send or forward e-mails containing libelous, defamatory, offensive, racist or obscene remarks
By sending or even just forwarding one libelous or offensive remark in an e-mail message, you and your agency can face legal charges resulting in multi-million dollar penalties.

Answer swiftly
Citizens and staff use an e-mail message because they wish to receive a quick response. Therefore, each e-mail message should be replied to within at least 24 hours, and preferably within the same working day. If the e-mail message is complicated, send a response that you have received their message and that you will get back to them.

Flaming
Avoid public "flames" – messages sent in anger. Wait and think about what you want to say before responding. Messages sent in anger only "fuel the flames" and are usually regretted later.

Do not attach unnecessary files
Wherever possible, only send attachments when they are productive and when necessary, compress the attachment. Large attachments can bring down an e-mail system.

Do not overuse the high priority option
We all know the story of the boy who cried wolf. If you overuse the high priority option, it will lose its function when you really need it. Moreover, even if an e-mail message has high priority, your message will come across as slightly aggressive if you flag it as 'high priority'.

Don't leave out the message thread
When replying to an e-mail message, include the original message in your reply--in other words click 'Reply', instead of 'New Mail'.

Do not overuse 'Reply To All'
Only use 'Reply to All' if you really need your message to be seen by each person who received the original message.

Take care with abbreviations and emoticons
In business e-mail messages, try not to use abbreviations such as BTW (by the way) and LOL (laugh out loud). The recipient might not be aware of the meanings of the abbreviations and these are generally not appropriate in business e-mail message. The same goes for emoticons, such as the smiley :-). If you are not sure whether your recipient knows what it means, it is better not to use it.

Be careful with formatting
Remember that when you use formatting in your e-mail messages, the sender might not be able to view formatting or might see different fonts than you had intended. When using colors, use a color that is easy to read on the background.

Take care with rich text and HTML messages
Be aware that when you send an e-mail message in rich text or HTML format, the sender might only be able to receive plain text e-mails. If this is the case, the recipient will receive your message as a .txt attachment.

Do not forward chain letters

Do not ask to recall a message
The chances are that your message has already been delivered and read. It is better to send a follow-up e-mail message to say that you have made a mistake. This will look much more honest than trying to recall a message.

Do not copy a message or attachment without permission
Do not copy a message or attachment belonging to another user without permission of the originator. If you do not ask permission first, you might be infringing on copyright laws.

Use a meaningful subject line
Try to use a subject line that is meaningful to the recipient as well as yourself. Often this is the only clue the recipient has about the contents when filing and searching for messages.

Use active instead of passive voice
Try to use the active voice wherever possible. For example, "Our department will contact you today" sounds better than "You will be contacted by our department today." The first sounds more personal and assures the recipient that you are actively working to meet their needs.

Avoid using URGENT and IMPORTANT
Even more so than the high-priority option, you must at all times try to avoid these types of words in an e-mail message or subject line. Only use this if it is a really urgent or important message.

Don't reply to spam
By replying to spam or by unsubscribing you are confirming that your e-mail address is 'live'. Confirming this will only generate more spam. Therefore, just hit the delete button or use e-mail software to remove spam automatically.

Use the "Cc:" field sparingly
Try not to use the "cc:" field unless the recipient knows why they are receiving a copy of the message. When responding to a "cc:" message, decide if you should include recipients listed in the "cc:" field as well. Generally, you do not include the person in the "cc:" field unless you have a particular reason for wanting this person to see your response. Again, make sure that this person will know why they are receiving a copy.

Signatures
Use a signature if you can. Make sure it identifies who you are and includes alternative means of contacting you (phone and fax).

Courtesy
E-mail is all about communicating with other people and as such remembering basic courtesies is never a bad idea. If you're asking for something, don't forget to say "please" and if someone does something for you, make sure you say "thank you."

How do you enforce email etiquette?
The first step is to create a written e-mail policy. This e-mail policy should include all of the do's and don'ts concerning the use of the company's e-mail system and should be distributed amongst all employees. Secondly, employees must be trained to fully understand the importance of e-mail etiquette. Finally, implementation of the rules can be monitored by using e-mail management software and e-mail response tools.

Chapter 7 - Case Study

As a city employee you have responsibilities for dealing with requests from the public. You are assigned to write a policy for content management of e-mail messages. What specific guidelines should you put in the policy?

No two organizations have the same business needs or mandates, therefore a perfectly acceptable policy for one organization may not work for another.

General recommendations for any organization should include responding in a timely and helpful manner; maintaining a professional tone at all times; striving for conciseness; avoiding sending frivolous messages or using network resources unnecessarily; avoiding slang or abbreviations; including all quoted material in the response; and not using e-mail messages for discussing sensitive topics, for delivering bad news, or for urgent business requiring an immediate response.

Finally, the policy should note that the law might see no distinction between e-mail sent from home or from work, and no distinction between the use of public equipment or private equipment when used for work purposes.

Chapter 7 - Quiz
True or False

1. **E-mail should be used for all forms of communication.**
   False. E-mail cannot replace personal contact. There is a tendency to be less formal or careful when communicating using e-mail and that can sometimes provoke anger. Remember that direct, person-to-person contact is best for handling sensitive, difficult, complex or emotional issues. In addition remember that e-mail is public. Don't say anything in an e-mail message that you would not want to be made public or forwarded to others. Never make any libelous, sexist or racially discriminating comments in an e-mail message and finally, e-mail should not be used to discuss confidential information. Sending an e-mail message is like sending a postcard. If you don't want your message to be displayed on a bulletin board, don't send it.

2. **The use of e-mail is considered "informal"; therefore it is acceptable to write in an informal style.**
   False. Because it is a business communication tool it is important to represent your agency in a professional manner which will help to protect your agency from liability and unnecessary risk.

3. **Because it is not on paper, it's okay to say what you really think about a co-worker in an e-mail.**
   False. It is never okay to use e-mail for libelous, sexist or racially discriminating comments about co-workers or any other individual for that matter. By sending or even just forwarding one libelous, or offensive remark in an e-mail message, you and your agency can face court cases resulting in multi-million dollar penalties.

4. **You should clearly identify the subject contained in your e-mail.**
   True. You should try to use a subject that is meaningful to the recipient as well as yourself. Often this is the only clue the recipient has about the contents when filing and searching for messages.

5. **It's not necessary to consider copyright laws when using attachments or forwarding messages.**
   False. Some messages and/or their attachments may have been copyrighted by their creator. Therefore, do not copy a message or attachment belonging to another user without permission of the originator. If you do not ask permission first, you might be infringing on copyright laws.

Sources

Compiled from the following sources:

www.Emailreplies.com, "Email Etiquette Rules For Effective Email Replies", November 3, 2003

Radcliff Community Email Committee, May 14, 2001.

Yale University Library, "Training & Staff Development Resources", January 20, 1999

E-Mail Rules: A Business Guide to Managing Policies, Security, and Legal Issues for E-Mail and Digital Communication, Nancy Flynn and Randolph Kahn, AMACOM (NY, NY) 2003.

The E-Policy Handbook: Designing and Implementing Effective E-Mail, Internet, and Software Policies, Nancy Flynn, AMACOM (NY, NY) 2000

Appendices

Appendix A

E-mail Policy Template

Note: *Agencies should pick and choose from this sample policy to suit their situation*

[Agency Name] has established this policy with regard to the acceptable use of agency-provided electronic messaging systems, including but not limited to e-mail and instant messaging. E-mail and instant messaging are important and sensitive business tools. This policy applies to any and all electronic messages composed, sent or received by any employee or by any person using agency-provided electronic messaging resources.

Policies

[Agency Name] sets forth the following policies, but reserves the right to change them at any time as may be appropriate or required under the circumstances.

- [Agency Name] provides electronic messaging resources to assist in conducting agency business.
- All messages composed and/or sent using agency-provided electronic messaging resources must comply with agency policies regarding acceptable communications.
- [Agency Name] prohibits discrimination based on age, race, gender, sexual orientation, physical or mental disability, sources of income, or religious or political beliefs. Use of electronic messaging resources to harass or discriminate for any or all of the aforementioned reasons is prohibited.
- The electronic messaging system(s) is (are) [Agency Name] property. All messages stored in agency-provided electronic messaging system(s) or composed, sent or received by any employee are the property of [Agency Name]. Furthermore, all messages composed, sent or received by any person using agency-provided equipment are the property of [Agency Name]. Electronic messages are NOT the property of any employee.
- Upon termination or separation from the agency, [Agency Name] will deny all access to electronic messaging resources, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.
- Each employee will be assigned a unique e-mail address that is to be used while conducting agency business via e-mail.
- Accessing external e-mail systems from agency-provided equipment is prohibited. This includes, but is not limited to, Yahoo! Mail, Hotmail, MSN Mail, AOL, Earthlink, Comcast and other e-mail services offered by Internet service providers.
- Employees are prohibited from automatically forwarding electronic messages sent through agency-provided systems to external messaging systems.
- [Agency Name] reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received. The interception, monitoring and reviewing of messages may be performed with the assistance of content filtering software, or by designated agency employees and/or designated external entities. Employees designated to review messages may include, but is not limited to, an employee's supervisor or manager and/or representatives from the Human Resources Department, Legal Department or IS Department.

- [Agency Name] reserves the right to alter, modify, re-route or block the delivery of messages as appropriate. This includes but is not limited to:
    - Rejecting, quarantining or removing the attachments and/or malicious code from messages that may pose a threat to [Agency Name] resources.
    - Discarding attachments, such as music, considered to be of little business value and of significant resource cost.
    - Rejecting or quarantining messages with suspicious content.
    - Rejecting or quarantining messages containing offensive language.
    - Re-routing messages with suspicious content to designated [Agency Name] employees for manual review.
    - Rejecting or quarantining messages determined to be unsolicited commercial e-mail (spam).
    - Appending legal disclaimers to messages.
- Electronic messaging resources may be used *infrequently* and *occasionally* for personal use. Excessive personal use may result in disciplinary action, including but not limited to the loss of this privilege and/or termination. [Agency Name]-provided electronic messaging resources may not be used for the promotion or publication of one's political or religious views, the operation of a business or for any undertaking for personal gain.
- [Agency Name] (does or does not) permit the use of instant messaging programs. The policies in this document apply equally to instant messages as well as e-mail.
- Employees authorized to use instant messaging programs will be advised specifically on which instant message program(s) are permissible and which ones are not.
- Employees authorized to use instant messaging programs will be assigned a unique instant messaging identifier, also known as a buddy name, handle or nickname.
- Employees are prohibited from conducting employee business from any non- [Agency Name] provided e-mail or instant messaging accounts.
- The unique e-mail addresses and/or instant messaging identifiers assigned to an employee are the property of [Agency Name]. Employees may use these identifiers only while employed by the [Agency Name]. The right to use these identifiers terminates upon termination or separation from the agency.
- [Agency Name] employs sophisticated anti-virus software. Employees are prohibited from disabling anti-virus software running on [Agency Name]-provided computer equipment.
- Any employee who discovers a violation of these policies should immediately notify a manager or the Human Resources Department.
- Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to, termination.

Practices and Procedures

[Agency Name] employs certain practices and procedures in order to maintain the health and efficiency of electronic messaging resources, to achieve agency objectives and/or to meet various regulations. These practices and procedures are subject to change as appropriate or required under the circumstances:

- [Agency Name] treats relevant electronic messages as a business record. As with any business record, established practices and procedures for the safekeeping, retention and ultimate destruction of the business record must be followed.

- [Agency Name] serializes, archives and retains copies of all internal and external electronic messages in conformance with retention periods outlined in the Archives Division's general records retention schedules.
- It is recommended that e-mail be printed when it contains information pertinent to a case file or important issue. The e-mail will then take on the retention period of that record series.
- _____ days after electronic messages have been successfully and verifiably archived, electronic messages will be deleted from the local, online electronic messaging system(s).
- The [Agency Name] automatically and systematically destroys all archived messages when the record has reached the end of its retention period as outlined in the Archives Division's general records retention schedule.
- In order to enforce the [Agency Name] retention schedules, employees are prohibited from copying or storing messages into any form of local message archive, including, but not limited to, PST (Outlook) files, public folders, personal folders and local file folders. Conflicts with guidance in chapter 3

Risks and Cautionary Advice

While electronic messaging resources allow employees to conduct agency business efficiently, use of e-mail and instant messaging systems comes with some inherent risks. All employees should be aware of these risks and take precautions to mitigate them.

- Electronic messages are legally discoverable and permissible as evidence in a court of law.
- Messages sent electronically can be intercepted inside or outside the agency and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through e-mail or instant messages.
- Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically instead of in person.
- Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
- Even though the agency employs anti-virus software, virus infected messages can could enter the agency's messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken:
    - Be suspicious of messages sent by people not known by you.
    - Do not open attachments unless they were anticipated by you.
    - Disable features in electronic messaging programs that automatically preview messages before opening them.
- Do not forward chain letters. Simply delete them.
- [Agency Name] considers unsolicited commercial e-mail (spam) a nuisance and potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These "Remove Me" links often are used by unscrupulous mass junk e-mailers as a means to verify that you exist. Attempting to remove yourself will only ensure that you will receive ever increasing amounts of spam.
- Internet message boards are a fertile source from which mass junk e-mailers harvest e-mail addresses and e-mail domains. Do not use agency-provided e-mail addresses when posting to message boards.

The undersigned acknowledges that he/she has received, read and understands the policies, practices, procedures, risks and cautionary advice that apply to [Agency Name] 's electronic messaging resources.

_____ _____

Employee Signature Date

Appendix B

GLOSSARY

Access – The right of any citizen to use public records as defined by ORS 192. See Also Public Records Act

Address Book – A list of e-mail addresses compiled by a user, sometimes with help from an e-mail system itself.

Administrative Value – The usefulness of a record to an organization in the conduct of its daily business.

Archives (noun) – (1) A place in which records selected for permanent preservation are kept, such as the Oregon State Archives. (2) A group of documents created or received and set aside by an agency or person during the course of their official business.

Archive (verb) – The practice of removing outdated information from and active environment to a remote storage environment. Archive, as a verb is essentially the action of managing electronic information.

Attachment – Any computer file (word processing, database, image, etc.) intentionally associated with, and received as part of an e-mail message.

Backup – A copy of electronic records and data that are retained to protect an organization against loss of the information. Backups can be stored on disks, tapes, or other machine-readable media. There are essentially two types of backups–security (See Backup, Security) and retention (See Backup, Retention).

Backup, Retention – A copy of electronic records and data that are retained to satisfy the retention requirements of the agency's records. Retention backups are kept for the entire length of the longest retention period specified for the information backed up.

Backup, Security – A copy of electronic records and data that are retained to protect an organization against loss of the information. Security backups are done on a regularly scheduled basis, can be partial or full backups and the tapes are re-used at the end of the scheduled backup cycle.

Chat Room – An online network discussion platform to encourage and manage online text discussions over a period of time among members of special interest groups or project teams.

Classification – The systematic identification and arrangement of records into categories according to logically structured conventions, methods, and procedural rules, represented in a scheme or plan.

Collaborative – Two or more people working together in real-time over a network or phone line using applications to share documents or videoconference.

Confidential Record – See Exempt records.

Convenience Copy – An unofficial copy of a record maintained for ease of access and reference.

Correspondence – Records that: 1. document communications created or received by an agency AND 2. directly relate to an agency program or agency administration AND 3. are not otherwise specified in the City General Records Retention Schedule (OAR 166-200), County and Special District General Records Retention Schedule (OAR 166-150) or in any agency special schedule or in ORS 192.170. Records may include but are not limited to letters, memoranda, notes and electronic messages that communicate formal approvals, directions for action, and information about contracts, purchases, grants, personnel and particular projects or programs. *Disposition:* File with the associated program or administrative records. Retentions for records can be found in the City General Records Retention Schedule (OAR 166-200) or the County and Special District General Records Retention Schedule (OAR 166-150). Communications not meeting the above criteria do not need to be filed and may be retained as needed.

Data Management – A major function of operating systems that involves organizing, cataloging, locating, storing, retrieving, and maintaining data.

Debug – To delete, locate and remove errors from a program or malfunctions from a computer.

Delete – To remove but not necessarily destroy all or part of a computer file.

Destruction – The process of eliminating or deleting data, documents, and records so that the recorded information no longer exists.

Dial-up Access – See Remote Access

Digital Signature – A type of electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (a) whether the transformation was created using the private key that corresponds to the signer's public key and (b) whether the initial message has been altered since the transformation was made. See Also Electronic signature. (ORS 192.835(4))

Discovery – Compulsory disclosure of documents in the possession of the other party once a legal action has been initiated.

Discussion Forum – See Chat Room.

Disposition – An action that occurs once a record's retention period has expired. Possible actions include transfer to permanent storage at the State Archives or deletion (destruction).

Disposition Date – The date on which the records retention period for a given records series expires and the records shall be disposed of by transferring to the State Archives for permanent storage or by deleting the records from the system.

Download - The process of pulling information from one computer onto another.

Electronic Mail (e-mail) – The physical computer system used to create, send, receive, and file messages electronically. The term may also refer to the messages transmitted through such a system.
Electronic Mail (e-mail) Account – An individual e-mail user's mailbox and associated rights to use that mailbox.

Electronic Mail (e-mail) Address – The character string used to allow computer systems to route an e-mail to the intended recipient, usually consisting of a user name, the @ symbol, and a domain name (i.e. john.h.doe@state.or.us).

Electronic Mail (e-mail) Administrator – The person responsible for maintaining an e-mail system, including all mailboxes on that system.

Electronic Mail (e-mail) Message – See E-mail Messages

Electronic Record – A record created, generated, sent, communicated, received, or stored by electronic means. (ORS 84.004(7))

Electronic signature – An electronic sound, symbol or process attached or logically associated with a record and executed or adopted by a person with the intent to sign the record. See Also Digital signature. (ORS 84.004(8))

Electronic Storage – See online, nearline, and offline storage.

E-mail Messages – Electronic documents created, received, or sent by a computer system. Applicable to the contents of the communication, the transactional information and any attachments associated to such communication.

E-mail Servers – Change to Server and Mail Server – a computer or software program that supplies data and responds to requests from workstations over a network.

E-mail Systems – The electronic mail system provides the means for creating messages, transmitting them through a network, and displaying the messages on the recipient's workstation, personal computer (PC) or terminal.

Encryption – A security method that encodes information into plainly unintelligible text making it impossible for anyone without a 'key' to decode the information. See also Public Key and Public Key Infrastructure

End User – Anyone who uses an information system or the information it produces.

Exempt – Certain public records that are in whole or in part restricted from public access. Exempt records and conditionally exempt records are listed in ORS 192.

File – (noun) A collection of related records that are treated as a unit, sometimes used synonymously with "records series" and sometimes referring to the contents of one case or file folder.

File – (verb) To arrange documents into a logical sequence.

Filing System – A pre-defined plan using numbers, letters or keywords to identify and organize records in a systematic scheme.

Filter – To select certain items from an electronic folder or database by determining how they fit specific criteria.

Firewall – Hardware and software that control the flow of traffic in a computer network. They stop intruders and viruses, while allowing authorized users and applications to send data freely.

Fiscal Value – The usefulness of a record in documenting an organization's financial decisions and activities.

Flame – An angry or rude e-mail message.

Folder – An electronic receptacle used to store electronic files.

Forward – To send a received e-mail message onto someone else.

Freedom of Information Act (FOIA) – A federal act that entitles citizens of the United States access to federal agency records and to information about themselves contained in federal government files. FOIA is not applicable to state and local government records. See Public Records Act

Group List – A list of names and e-mail addresses organized into a group that enables the sender to enter only the group list name when sending a e-mail to the group of list members.

Hard Copy – A printed or paper copy of an electronic document.

Historical Value – The usefulness of a document in facilitating historical research.

Hypermedia –Documents containing multiple forms of media including text, graphics, voice and sound that can be interactively searched.

Inbox – The part of an e-mail system where a user's incoming messages are received.

Index – The process by which specific subject terms are associated or attached to records and information to facilitate its retrieval using search functions. May also refer to a list of subject terms for a particular body of records or information.

Instant Messaging (IM) – Is the ability to chat remotely with an ongoing exchange of short sentences. In addition to "chatting," IM allows for the direct transfer of data files; direct sending and receiving of messages to and from cell phones, pagers, telephones and fax machines; voice-over-IP (using your computer like a telephone); sending and receiving e-mail messages; web-conferencing, application sharing, and remote control of another computer; subscriptions to content channels (i.e. news, sports, weather, stocks, etc.); and monitoring when other parties are signed in to the IM system.

Intelligent Agent – A special purpose knowledge based system that serves as a software surrogate to accomplish specific tasks for end users.

Interface – A shared boundary between two systems.

Internet – The vast network of computer systems that enables worldwide connectivity among users and computers. See also Worldwide Web

Intranet – A closed network that uses technology to restrict web-based information to a group of authorized users.

Legal Value – The usefulness of a record to support an organization's business agreements and ownership rights, and to document the rights of citizens.

Listserv – A discussion group that uses e-mail to allow subscribers with common interests to communicate about topics that interest them. Listservs usually require that its members subscribe to the service and abide by a set of rules in order to participate.

Log-in – To begin a user session on a computer by authenticating one's identity usually by using a username and it's associated password.

Local Area Network (LAN) – A network within a limited geographic area (usually under one mile) that allows personal computers to communicate directly with one another and share data.

Magnetic Storage – A type of digital storage that includes magnetic disks and tapes that stores the programs and files used daily. Magnetic storage provides random (disk) or sequential (tape) access and are a common choice for long-term, high capacity storage.

Mailbox – An area in an e-mail system where a single user stores messages received, sent, and trashed and composes outgoing messages. User may be able to transfer messages between the mailbox and additional message storage areas.

Mailing List – An automated list of e-mail addresses used to distribute e-mail messages to a number of people at the same time. See also Group List.

Mail Server – A computer that provides e-mail services to other computers in the network.

Mass Storage – Applications, such as imaging and processing-intensive operating systems, that allow large amounts of information to be stored offline.

Media – All tangible objects on which data are recorded.

Message Retention – Method of storing and retaining incoming and outgoing e-mail messages.

Message Store Management – Method of temporarily storing messages for later transmission to one or more recipients.

Metadata – Data that describes data including subject, date, and recipients of an e-mail.

Migration – The periodic transfer of data from one electronic system to another that retains the integrity of the data and allows used to continue to use the data despite technological advances in the hardware and software used to access the data.

Mission-critical Information – Information critical to the survival of an organization, such as charters, council records, etc.

Near-line Storage – The storage of e-mail messages, metadata, and attachments in an electronic record keeping system. This type of storage requires that the messages, metadata, and attachments be removed from the online email system and stored in an electronic format. Near-line storage allows the user to maintain a moderate amount of functionality, in that email messages stored near-line can be retrieved and referenced electronically.

Needs Assessment – A report that systematically examines a records management problem, evaluates solutions, and recommends a solution.

"Netiquette" – Network etiquette. The acceptable practices for online communications.

Network – A system of computers and related devices interconnected so that they can communicate together.

Off-line Storage – The storage of e-mail messages, metadata, and attachments of an electronic record keeping environment. The clearest example of this type of storage is to simply print out an email message to paper. Off-line storage reduces the functionality of the message in that it is no longer available electronically.

On-line Storage – The storage of e-mail messages, metadata, and attachments in the e-mail system that is being used at an agency.

Password – A character string usually selected by the user that is known to the computer system and used in conjunction with an associated user name to identify the user and allow access to the system.

Personal Digital Assistant (PDA) – Hand-held microcomputer devices that enable you to manage information such as appointments, to-do lists, contacts, send and receive e-mail, access the Worldwide Web, and exchange such information with your personal computer or network server.

Policy – A broad document that specifies a general rule for records and information management in an organization. A plan or course of action, as of a government, political party, or business, designed to influence and determine decisions and actions; a *course of action, guiding principle, or procedure* considered to be expedient, prudent, or advantageous.

Procedure – A detailed document that specifies step-by-step rules for records and information management in an organization.

Proprietary Software—Privately owned and controlled software. In the computer industry, proprietary is the opposite of open. It also implies that the company has not divulged specifications that would allow other companies to duplicate or customize the product.

Protocol – The definition of specific rules two or more computers will follow when communicating.

Public Record – Includes, but is not limited to, a document, book, paper, photograph, file, sound recording, or machine-readable electronic record, regardless of physical form or characteristics, made, received, filed, or recorded in pursuance of law or in connection with the transaction of public business, whether or not confidential or restricted in use. Public record does not include: (a) records of the Legislative Assembly, its committees, officers, and employees; (b) library and museum materials made or acquired and preserved solely for reference or exhibition purposes; (c) records of information concerning the location of archaeological sites or objects…; (d) extra copies of a document, preserved only for convenience of reference; (e) a stock of publications; (f) messages on voice mail or on other telephone message storage and retrieval systems. (ORS 192.0052(5))

Public Records Act – Located within ORS 192, this Act grants the public the right to inspect public records with the exception of certain records listed in the act. The Act states "every person has a right to inspect any public record of a public body in this state, except as otherwise expressly provided by ORS 192.501 to 192.505." (ORS 192.420)

Queue – A structure that organizes e-mail messages in a predetermined order such as when they are received or who sent them.

Realtime – Pertaining to the performance of data processing during the actual time a business or physical process transpired in order that results of the data processing can be used to support the completion process.

Recipient – A person who receives an e-mail message.

Record – See Public Record

Record Series – Records arranged according to a filing system or kept together because they related to a particular subject or function or result from the same activity.

Records Management – The planning, controlling, directing, organizing, training, promoting and other managerial activities relating to the creation, maintenance, use, access and disposition of records.

Records Officer – An individual, designated by the agency to work directly with the State Archives on records related issues and to coordinate and implement sound records management principles and practice within their agency.

Records Retention Period – The length of time that messages and attachments must be kept before they are destroyed or otherwise disposed of.

Records Retention Schedule – A document that lists records and how long they should be kept.

Recovery – How a computer system resumes operation after experiencing a problem with the hardware or software used to operate the system.

Remote Access – Pertaining to communication with the data processing facility by one or more stations that are distant from that facility.

Reply – To respond to an e-mail message.

Retention – The length of time that messages and attachments must be kept before they are destroyed or otherwise disposed. See also Records Retention Period.

Routing – The path used to transmit an e-mail message over a network.

Security – The protection of records an information by controlling which users can access which documents and for what purpose.

Sender – A person who transmits an e-mail message.

Server – See Mail Server

Signature Line – A set of usually four to eight lines of text placed automatically by an e-mail system at the end of an outgoing e-mail message to provide the reader with the sender's contact information.

Software – Programs that run operations on a computer

Spam – An unsolicited e-mail message.

Storing – Process in which information is recorded and retained for later retrieval. See Also Offline, Nearline, and Online Storage.

Systems Administrator – The person responsible for maintaining a computer system such as a local area network (LAN) or an e-mail system.

Technological Obsolescence – The tendency for any component of computer technology (hardware, software, and data formats) to become unusable as time goes on because all of the necessary components that allows the system to work together are no longer available in the new computing environments.

Text File – A computer file that contains nothing but ASCII text and formatting and therefore can be read by many different types of computer programs.

Transport Control Protocol/Internet Protocol (TCP/IP) – The basic communications system that allows communication between computers via the Internet.

Trojan Horse – An apparently harmless set of computer code that sneaks a virus onto a computer system.

Uniform Resource Locator (URL) – The location or address of a resource on the Internet (i.e. http://arcweb.sos.state.or.us)

Username – The name used to identify a user of a computer system, usually some abbreviation of the person's name and used in conjunction with a password to verify the user's identity.

World Wide Web (WWW) – The portion of the Internet that supports the presentations of information formatted in HTML, including hyperlinks so users can move quickly to other resources.

Worm – A type of computer virus that spreads itself usually by creating copies of itself in each computer's memory.

Vital/Essential Record – A record that is essential to the organization's operation or to the re-establish business operations after a disaster. See also Mission Critical Information.

Appendix C

E-mail Policy Training
Example from the City of Tigard

E-mail Policy Training

for
The City of [your city]

Who does this policy apply to?

This policy applies to all City of [city name] employees and their use of the city's electronic mail (e-mail) system.

It is the City's goal to enhance both external and internal communications through the use of various electronic communication tools.

All electronic communication tools are the property of the City of [city name].

Any individual using the e-mail system is subject to monitoring and all individuals using the system without authority or in excess of their authority are subject to having all their activities on this system monitored, recorded and examined by an authorized person, including law enforcement, as system personnel deem appropriate.

The 1986 Electronic Communications Privacy Act allows employers to monitor employees' electronic information at their discretion.

Users understand that the City may use automated software to monitor material created, stored, sent, or received on its computer network.

Personal Use

The personal use of City computers, *with the exception of e-mail and the Internet*, is permitted:

- during an employee's lunch period,
- one hour before or after their normal work schedule begins or ends, and
- the time between the end of the employee's "work shift" and the beginning of an evening meeting that the City requires the employee to attend.

Personal use of the e-mail system and the Internet is not allowed at any time.

E-Mail

The City's e-mail system may not be used:

- To access an employee's personal internet e-mail account.

The City of [city name] has Internet access computer stations available for use. Sign up to use a station during breaks, lunch, or after work hours.

E-Mail (Cont.)

The City's e-mail system may not be used:

- To forward another's email without the originator's permission.

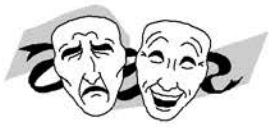
Gain the permission of the originator before sending your e-mail on.

E-Mail (Cont.)

The City's e-mail system may not be used:

- To send e-mail anonymously or under someone else's name.

Occasionally, an employee may need to use another employee's e-mail (the switchboard is a good example). Simply identify yourself at the beginning of the message.



E-Mail (Cont.)

The City's e-mail system may not be used:

- To support charitable, religious, or political activities or causes.

Some examples are: United Way, Special Olympics, Relay for Life, and Walk for Diabetes.

E-Mail (Cont.)

The City's e-mail system may not be used:

- To support other activities that are not related to the direct conduct of City business.

The City agrees that the Union may utilize the inter-office e-mail system as another form of communication between employees. (Article 6, Section 3 of the Collective Bargaining Agreement between the City of Tigard and the SEIU Local 503/OPEU Local 199).

The Union agrees that the e-mail system will not be used to discuss negotiations or to transmit confidential material such as grievance information.

Employee Responsibility

If an employee receives an inappropriate e-mail, respond to the sender with the warning message found in I:\citywide\Email-WARNING.doc and notify your supervisor.

Employee Responsibility (Cont.)

If an employee receives a personal e-mail, he or she must immediately respond to the sender with a message notifying the sender the employee may not receive personal e-mail at the City.

An example is available at: I:\citywide\personale-mail.doc

Laws and License Compliance

Users are required to comply with all software licenses, copyright laws, Oregon Government Standards and Practices Commission's guidelines, and City policies when sending or receiving e-mail or accessing or downloading information from the Internet.

System Security

All employees have a responsibility to take reasonable precautions to protect the City's computer system.

If an employee becomes aware of a virus or the threat of a virus, the employee should immediately contact Network Services with the information. Network Services will evaluate the risk.

Electronic Mail Can Be a Public Record!

Under Oregon's public records law, most e-mail messages are clearly public records.

The definition of public records "includes, but is not limited to, a document, book, paper, photograph, file, sound recording, machine readable electronic record regardless of physical form or characteristics, made, received, filed or recorded in pursuance of law or in connection with the transaction of public business, whether or not confidential or restricted in use."

If you don't want it printed on the front page of the [Local Paper] Times...

You don't want to put it in an e-mail.

A person need not have a "legitimate" need for public records to be entitled to inspect them.

The City's Public Access to City of [city name] Records policy is available online at:

http://www.ci.tigard.or.us/city_hall/services/public_records

Please check with your supervisor, or Records, if you have a question on whether an electronic mail message should be released.

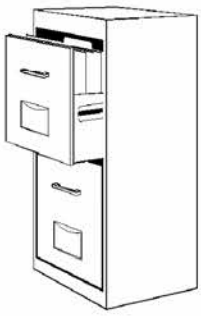
City employees bear any responsibility that might arise from use of the computer system for personal or improper reasons.

Retention and Disposition

The retention of records stored in electronic records systems, including e-mail, is governed by the City's retention schedule. If you have a question on the retention of a message, please contact the Records Section.

IF IN DOUBT, PRINT IT OUT!

An e-mail mailbox should not be used for storage. E-mails are deleted from your mailbox after six months by Network Services. If an e-mail has value it should be printed and put into the appropriate file. It is the responsibility of the holder of the official record to make sure the file is updated.



Archiving E-Mail

E-mail can be saved for longer than six months if it is selected for archiving. For instructions on archiving your e-mail go to the "Records" folder in the I Drive, Select the "Email" folder, select the "Archived Email" folder, and open "Archive Instructions".

E-mail related to a current project or issue may be retained on the system as a reference tool.

Once the project is completed or the issue resolved the employee should verify all relevant e-mail is on the file and then deleted the e-mail from their e-mail box.

Again, if your e-mail falls within the definition of a public record, you may not delete it except as provided in the City's retention schedule.

This concludes the City's Computer Use, E-mail, and Internet Policy Training

Please sign the form at the back of your handout. This form is an ***acknowledgment*** that you understand the City of [city name] policy.

If you have other retention related questions, you may contact the Records Section at extension 359.

COMMITTEE	MEMBER/TERM	APPOINTMENT PROCESS/AUTHORITY	ELECTED REPRESENTATIVE REQUIRED?
Metro Joint Policy Advisory Committee on Transportation (JPACT)	Councilmember Peterson (Lake Oswego) is the member and Mayor Bernard is the alternate.	Section 2.19.090(b) of the Metro Code and Article IV of the JPACT By-Laws establish the JPACT membership. There are 17 members. There is one city representative and one alternate from Clackamas County. The member and alternate must be from different cities. Selection of the member and alternate is by the cities within the county. The term of appointment is for two years.	Yes
Metro Policy Advisory Committee (MPAC)	No appointee from the Milwaukie City Council. Mayor Lehan (Wilsonville) is the member and Mayor King (West Linn) is the alternate.	Section 26 of the Metro Charter establishes the MPAC membership. There are 28 members. There is one member and an alternate from the largest city in Clackamas County. That member is selected by that jurisdiction. There is an additional member selected by the remaining cities within Metro's boundaries in Clackamas County. That member and alternate are selected by those cities.	Yes
South Corridor Policy Committee (SCPC)	Mayor Bernard	The SCPC was created by the Metro Council for a specific purpose/project. It therefore does not have by-laws or a term of office. The Mayor has been the City's appointee.	Yes
Clackamas County Coordinating Committee (C-4)	Mayor Bernard	Section 2 of the By-Laws of the C-4 provide that the "voting membership" be an "elected representative or an alternate appointed by the City Council . . .."	Yes
North Clackamas Parks and Recreation District Urban Parks Advisory Board (UPAB)	Mart Hughes	Section E(2) of the May 1, 1990 Agreement between Clackamas County and the City provide for the UPAB. The City Council appoints the UPAB	No

		member. With the exception of the Milwaukie representative, UPAB members are appointed for 3 year terms. The term for a Milwaukie appointee is up to the City Council. The current appointee has served for 4 years.	
Johnson Creek Watershed Council (JCWC)	JoAnn Herrigel	Article III, By-Laws, authorizes a council of 3 to 40 members. By separate resolution the Council established groups from which it would seek representation, including the City. The City Council appoints the member.	No
Regional Water Providers Consortium	Councilmember Collette is the member and Mayor Bernard is the alternate.	The term is at the discretion of the City Council.	Yes
Regional Partners	Kenny Asher is the member and Mayor Bernard and Alex Campbell are the alternates.	The Regional Partners provide a forum for the regional discussion of economic development issues.	No