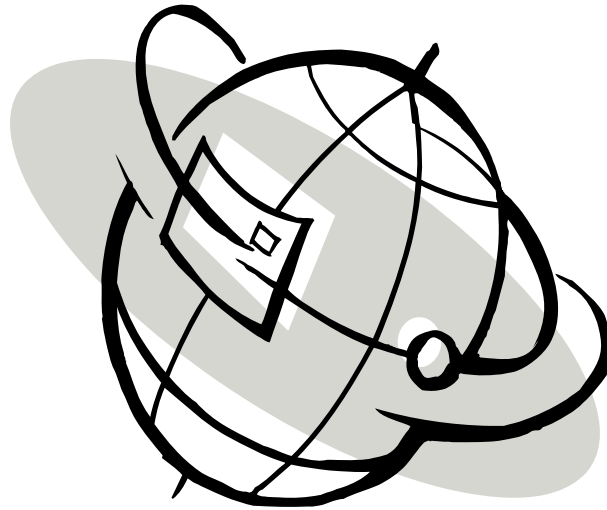


EMAIL @CITY-HALL.COM

Email Issues for City Officials



**Including Etiquette, Open Government,
& Other Legal Issues**

UPDATED AND PRESENTED BY:

HELEN VALKAVICH

*Assistant City Attorney
City of San Antonio
210-207-8992
helenv@sanantonio.gov*

***AUTHORED BY:
SCOTT HOUSTON***

*Legal Services Director
Texas Municipal League
512-231-7400
shouston@tml.org*

Presented to:

Texas City Attorneys Association
Semi-Annual Summer Conference
South Padre Island, Texas
June 11, 2004

TABLE OF CONTENTS

I. Introduction.....	5
How Email Works	5
II. Email Etiquette..	6
Introduction	6
Golden Rules	6
Format.....	6
Forwarding.....	7
Carbon Copy.....	7
Personal Information	8
Return Receipt Request.....	8
Angry Email... ..	8
Attaching Files.....	8
Email is Not a Fact of Life Yet.....	8
III. Legal Issues.....	8
Public Information Act.....	8
Introduction.....	8
Member of the Public’s Email Address Confidential.....	9
Officer or Employee’s Email Address Generally Public.....	10
Email Request for Public Information	11
Email as Public Information.....	11
Home Email as Public Information	11
Exceptions to Disclosure	15
Records Retention	16
Records Retention Schedule.....	16
Email No Longer in Existence	16
Deleted Email.....	16
Destroying Public Information	18
Conclusion and Suggestions.....	18
Open Meetings Act.....	19
Introduction.....	19
Other Jurisdictions	20
Telephone Conversations, Letters, and Email.....	21
Agenda Setting.....	24
Aiding and Abetting	24
Conclusion and Suggestions.....	25

Sexual Harassment	25
Attorney-Client Relationship	26
Confidentiality.....	26
Lawyer-Client Privilege	26
Privacy Issues	28
Introduction.....	28
Fourth Amendment	29
Electronic Communications Privacy Act.....	29
Invasion of Privacy	30
Conclusion.....	30
IV. Conclusion.....	31
V. Sample Forms and Policies	31
City of Arlington Email Tips	32
City Council Email Retention Guidelines	33
TSLAC Model Email Policy	34
Sample Computer Use Policy	40

I. INTRODUCTION

Few new workplace technologies have found such widespread and rapid acceptance as electronic mail (email). However, email is still a relatively new form of communication, and - as is often the case - the law sometimes lags behind the ever-developing technologies in the modern world. Compliance with the many laws that affect a city official is confusing and difficult, especially when dealing with emerging technological issues such as email.

This paper focuses specifically on email issues; including etiquette, open government, sexual harassment, privacy, and the attorney-client relationship. The Texas Municipal League (TML) also has others available on topics mentioned herein, including but not limited to sexual harassment and open government.

This paper would not have been possible without the help of Alan Bojorquez, Bovey, Akers and Bojorquez; and Jay Doegey, City Attorney, Elizabeth Lutton, Senior Attorney, and Linda Frank, Assistant City Attorney - all of the City of Arlington.¹

How Email Works²

What is e-mail? In its simplest form, e-mail is an electronic message sent from one computer to another. Just as a letter makes stops at different postal stations along its way, email passes from one computer, known as a mail server, to another as it travels over the Internet. Once it arrives at the destination mail server, it is stored in an electronic mailbox until the recipient retrieves it. This whole process can take seconds, allowing for quick communication with people around the world at any time of the day or night. To receive email, a person must have an account on a mail server. This is similar to having an address where you receive letters. Once you connect to your mail server, you download your messages.

To send email, you need a connection to the Internet and access to a mail server that forwards your mail. The standard protocol used for sending Internet email is called Simple Mail Transfer Protocol (SMTP). It works in conjunction with Post Office Protocol (POP) servers. When an email message is sent, the computer routes it to an SMTP server. The server looks at the email address (similar to the address on an envelope), then forwards it to the recipient's mail server, storing it until the addressee retrieves it.

¹ Much of the open government information in this paper is based on an article written by Jay Doegey and Elizabeth Lutton for the International Municipal Lawyers Association magazine entitled "*To: Council Members, Re: You've Got Email, Message: Think Before You Reply,*" from the Municipal Lawyer, January/February 2002, Vo. 43, No. 1.

² How on earth is a lawyer supposed to answer that?! All of the information in this section of the paper is taken from <http://www.webfoot.com/advice/email.top.html?yahoo>, which is the simplest explanation I could find. As far as I know, email is transferred by little green elves.

II. EMAIL ETIQUETTE

INTRODUCTION

The following tips have been collected and combined from several sources, including personal experience and various Internet websites.³ The information below is intended as a guide for work-related email. The tips may or may not apply to personal use of email and certainly do not constitute legal advice.

Probably the most important lesson, which applies regardless of possible legal liability, is to never put anything in an email that you do not want the world to know about. Emails can be saved, forwarded, and - most importantly - are a permanent record that can be produced at a later date.

GOLDEN RULES

Format

A sender of email should always:

- 1) spell check email and use proper punctuation and grammar;
- 2) open email with a salutation and end with a closing and/or signature;
- 3) thank the recipient in advance if requesting help or information.

It reflects poorly on the sender when an email is sloppily drafted. A thoughtfully drafted email is a strong indication of education and professionalism. Of course, email sent to an employer or customer may be more formal than to a colleague or friend. Each individual will need to determine the appropriate format based on the recipient and topic of the email.

Do not type messages in all capitals. This is considered yelling or screaming online. Refrain from formatting your emails by bolding text or adding pretty colors and backgrounds. Some older email programs may not be able to read your email if you do. In addition, recipients of your email may not appreciate your design style, and colors and fancy text often make an email difficult to read.

Finally, because it is impossible to incorporate verbal and nonverbal communications that normally accompany the spoken word into email, do not forget that eye contact, tone of voice, and body language that we take for granted when communicating in person is not available in the written word. The lack of these cues in email can easily lead to misunderstanding.

³ See e.g., <http://www.onlinenetiquette.com/index.html>; <http://www.dynamoo.com/technical/etiquette.htm>; http://www.findarticles.com/cf_dls/m6280/6_186/53462131/p1/article.jhtml.

Forwarding

Do not ever, ever, for any reason whatsoever, forward to work colleagues⁴:

- 1) joke emails;
- 2) religious emails;
- 3) virus warnings;
- 4) chain letter emails; or
- 5) anything not work-related.

Why? First, most people have seen the funny joke or special offer at least fifty times before receiving it from you. Second, people often do not have time to look at this type of material at work. Third, it reflects on your professionalism. Fourth, forwarding these so-called humorous emails may offend or upset people who do not share your sense of humor or who are sick and tired of having to sort through an “in” box full of worthless, junk, emails. Fourth, joke emails may implicate some of the legal issues discussed later in this paper. Finally, many “virus warnings” actually contain a virus themselves. Thus, when you forward the warning to all your friends, you are actually sending them a virus. Rely on your virus protection software instead.

If you must forward a message, refrain from simply hitting “forward” and sending the message without an explanation. Always include a personal message about why it is important to the recipient and what, if any, action the recipient should take. Do not be afraid to respond to a “chronic forwarder” to tell them your preference to not receive forwarded emails of any nature. Cite company policy, warn them of the legal ramifications, or simply tell them that you like to hear from them personally, but not solely because they thought you might like a joke that they read.

Also, always ask permission prior to forwarding another person’s email.

Carbon Copy

A long list of email addresses at the beginning of an email is an immediate sign that the sender does not respect the privacy of those on the list. To some people, an email address is like their phone number. Only the owner of the email address or phone number is the one to authorize whom they want to have it and whether it should be made public. Many people prefer to decide for themselves who has their email address.

By sending a mass email to a list of recipients, you have decided for everyone on the list that everyone else on the list should have their email address. When it is necessary to send the same email to many recipients, the recipients should be listed in the Blind Carbon Copy (BCC) field. A recipient whose address is listed in the BCC field will receive a copy of the email, but their address cannot be seen by other recipients.

⁴ Can you tell that I am fed up with forwarded emails?

Of course, if you are emailing a group of trusted colleagues and want each recipient to be aware of who is being copied with the email, the above advice does not apply.

Personal Information

Never give out personal contact information of others without their specific permission to do so.

Return Receipt Request

Return Receipt Request (RRR) feature should only be used when it is critical to knowing when an email has been opened. RRR should not be used simply because you like to know when someone opens the email you sent. The RRR feature is often annoying and intrusive, and it should not be used as a matter of routine. For example, consider whether you would want someone who left you a voicemail message to know exactly when you listen to it.

Angry Email

When using email for work-related purposes, it is inevitable that city officials will receive angry, rude, or abrasive emails. Because people are not communicating face-to-face with email, they are often very bold when using this method of communication. If it is necessary to respond, do so in a courteous and professional manner. If it is not, do not respond.

Attaching files

Be aware of who the recipient of an email is and their system capabilities. For those who are lucky enough to have a T-1, cable, or DSL connection, large files do not generally represent a problem. However, for those using a dial-up connection, a file that might take ten seconds for a T-1 connection might take up to thirty minutes to download.

Email is Not a Fact of Life Yet

Many people have email addresses, but some do not regularly check their mailboxes. Do not assume that, because an email address appears on a business card, a person regularly reads his or her email. To avoid confusion, make sure your recipients are comfortable receiving e-mail.

III. LEGAL ISSUES

PUBLIC INFORMATION ACT

Introduction

The Texas Public Information Act (TPIA) gives the public the right to request access to government information. The preamble declares the purpose of the TPIA:

Under the fundamental philosophy of the American constitutional form of representative government that adheres to the principle that government is the servant and not the master of the people, it is the policy of this state that each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees. The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may retain control over the instruments they have created. The provisions of this chapter shall be liberally construed to implement this policy.⁵

The TPIA defines “public information” as information that is collected, assembled, or maintained by or for a governmental body.⁶ Under the definition, virtually every form of information is covered, including information recorded on, among other things, paper, film, tape, or a magnetic, optical, or solid state device that can store an electronic signal (e.g., a computer disk, hard drive, or other memory storage device).⁷

Texas, like many other states, recognizes that work-related email is information that may be subject to public disclosure.⁸ Thus, caution should be used when drafting and/or transmitting email. The following sections provide a discussion of the many pitfalls a city official may encounter under the TPIA when using email.

Member of the Public’s Email Address Confidential

Section 552.137(a) of the TPIA provides that an email address of a member of the public used for the purpose of communicating with a governmental body is confidential and not subject to disclosure.⁹ This means that the government must seek to protect this information, unless the member of the public has affirmatively consented to its release.

Section 552.137 was amended in 2003 to clarify this exemption does not apply to certain types of email addresses, particularly addresses of those individuals doing business or seeking to do business with the government and email addresses listed on documents intended for the public’s information. Section 552.137(b) states that subsection (a) does not apply to email addresses:

⁵ TEX. GOV’T CODE § 552.001(a).

⁶ *Id.* at § 552.002(a).

⁷ *Id.* at § 552.002(b).

⁸ See Fla. Op. Att’y Gen. 34 (1996)(Email made or received in connection with transaction of official business is public record as defined by Fla. Stat. Ann. § 119.011(1) (1996)); Maryland Op. Att’y Gen. 016 (1996)(Email related to conduct of public business is subject to Maryland Public Information Act).

⁹ See, e.g. Tex. Att’y Gen OR2001-6127.

- 1) of a person who has a contractual relationship with the governmental body or by the contractor's agent;
- 2) provided by a vendor who seeks to contract with the governmental body or by the vendor's agent;
- 3) contained in a response to a request for bids or proposals, contained in a response to similar invitations soliciting offers or information relating to a potential contract, or provided to a governmental body in the course of negotiating the terms of a contract or potential contract; or
- 4) provided to a governmental body on a letterhead, coversheet, printed document or other document made available to the public.

Section 552.137(d) further provides that a governmental body may for any reason disclose an email address to another governmental body or federal agency.

Internet website and general business email addresses, though, are not excepted from disclosure under these provisions.¹⁰

Officer's or Employee's Email Address Generally Public Information

While the email addresses of members of the public may be confidential, email addresses of government officers or employees are not protected by §552.137, nor are they automatically protected under other provisions.¹¹

However, city officers or employees have some protection under § 552.117 of the TPIA. That provision excepts from disclosure the home address, telephone number, social security number, and family member information of a current or former official or employee of a governmental body who requests that this information be kept confidential under § 552.024. The attorney general's office has "read this exception to include the home e-mail addresses of government officials or employees as well."¹²

Section 552.024 requires an officer or employee to request confidentiality within fourteen days of being hired, appointed, elected, or leaving employment, unless the person is a peace officer.¹³ However, an employee may later amend this decision so long as no request for the information is pending.¹⁴ A sample form for officers or employees to elect confidentiality is included in an appendix to this paper.

¹⁰ Tex. Att'y Gen. OR2004-0526.

¹¹ Tex. Att'y Gen. OR2003-3627; Tex. Att'y Gen. OR2001-4694; Tex. Att'y Gen. OR2001-4624.

¹² Tex. Att'y Gen. OR2001-4560 (concluding that home email address may be withheld pursuant to §§ 552.117 & 552.024 - *but citing no precedent for that conclusion*). See also Tex. Att'y Gen. OR2000-4906.

¹³ Senate Bill 247, passed in 2001, makes identifying information concerning a peace officer as listed in TEX. GOV'T CODE § 552.117 automatically confidential, regardless of whether the officer has elected to keep the information confidential.

¹⁴ Tex. Att'y Gen. ORD-530 (1989).

Email Requests for Public Information

Section 552.301(c) of the TPIA provides that a written request for information may be submitted by email or facsimile.¹⁵ To be effective, an email or facsimile request must be submitted to the officer for public information or the person designated by the officer. The chief administrative officer of a governmental body is the officer for public information.¹⁶ Depending on the city, the chief administrative officer under the statute may be the mayor, city manager, city administrator, or city secretary. In any case, a city should designate a public information officer to avoid any confusion as to who is responsible for responding to any request, including email or facsimile requests.

Email requests for information can be problematic. The first issue, mentioned above, is to whom the request must be addressed in order to invoke the deadlines under the TPIA. Next, the question of when a request is received is important. Under § 552.301, a properly addressed email request for information starts the clock tolling on the day that it is received by the city. Thus, the date that the officer for public information or the officer's designee first checks his or her email and sees the request is irrelevant.¹⁷ In other words, a city cannot claim that it received a request when the email was opened. Rather, the email is received on the day it arrives at the appropriate computer - usually the same day it is sent by the requestor, regardless of whether it is received after business hours. In light of the above, it is imperative to have procedures in place to avoid missing the statutory deadlines.

At least one state agency has adopted procedures that only authorize email requests to be sent through a special request page on the agency's website.¹⁸ This procedure is arguably allowable under § 552.230 of the TPIA, which empowers governmental bodies to promulgate reasonable rules of procedure with respect to obtaining public information.

Email as Public Information

The TPIA applies to electronically generated documents.¹⁹ Since email communications are a form of electronically generated document, email communications generated or received by city officials may become the subject of a public information request, just like other written correspondence. A request for email should be analyzed and handled in the same way as any other request for printed or written documents.

Home Email as Public Information

The attorney general's office has recognized that work-related email is public information subject to the TPIA. This recognition, by itself, is not too alarming.

¹⁵ Added by House Bill 951 (1997).

¹⁶ TEX. GOV'T CODE §552.201(a).

¹⁷ Tex. Att'y Gen. OR2001-1755.

¹⁸ The Texas Department of Transportation requires email requests to be submitted through its Internet website pursuant to 43 T.A.C. § 3.12(a)(1)(B).

¹⁹ TEX. GOV'T CODE § 552.002.

After all, other types of correspondence that do not fall within a statutory exception to disclosure are public.

More troubling is the fact that the attorney general, broadly interpreting the TPIA, concluded that home email sent to or from a personal computer through a private email account may be public information.

In 2001, the City of Arlington received a request for any city-related emails on any computer used by an Arlington city councilmember. The city released the emails from the councilmember's city email account, but requested an attorney general opinion as to whether the emails maintained in the councilmember's home computer were required to be released.

The city - along with supporting comments filed by the Texas Municipal League (TML) - argued that, even though the councilmember used her home computer email account to interact with her constituents and others, the fact that no city funds were used to pay for the email account or the computer, coupled with the fact that the emails were not held by the city, meant that the emails were not public information as defined by the TPIA.

Section 552.002(a) of the TPIA defines public information as "information that is *collected, assembled, or maintained under a law or ordinance* or in connection with the transaction of *official business*:"

- (1) *by a governmental body; or*
- (2) *for a governmental body and the governmental body owns the information or has a right of access to it.*

The city and TML argued that a councilmember's home emails are not collected, assembled, or maintained by the governing body of a city, nor does the governing body of a city own or have a right of access to such emails. Neither the City of Arlington's records control schedule, nor the city's charter, required the retention of this type of information. The emails were not required to be maintained by the city, nor could the city require their disclosure.

Further, the city and TML argued that § 552.001 of the TPIA states that the public is only entitled to information regarding the "affairs of *government* and the *official acts of public officials*." As quoted above, § 552.002(a) defines public information as related to "official business." An individual councilmember is not the government, nor are communications with constituents on a personal level "official acts" or "official business." As the attorney general's office stated in Open Records Decision No. 225, "[t]he governing authorities of representative bodies such as cities...can act only in meetings duly assembled and conducted,

and only through properly recorded minutes of their operations.”²⁰ Thus, it should be axiomatic that the members of local governing bodies can perform no official act except as part of a body at meetings properly convened and conducted.

The use of email exchanges to gain personal insight into the views of citizens is the modern-day equivalent to visiting on the phone or in person with a constituent. To conclude that personal emails of a councilmember are open for all to view has a chilling effect on the willingness of elected officials to explore and seek to understand the issues that are important to their constituents.

In sum, the city and TML argued that because the email messages in question were not collected, assembled or maintained by or for a governmental body, the governmental body did not own the emails, or have access to them, and the act of writing the emails was not an “official act” or “official business” of the councilmember, the email messages should not be considered public information subject to the TPIA.

The attorney general’s office disagreed.²¹ In a May 2, 2001 opinion, the attorney general’s office concluded that information is generally “public information” when it relates to the official business of a governmental body or is maintained by a public official or employee in the performance of official duties, *even though it may be in the possession of one person*. Citing the preamble of the TPIA, the opinion states that “it is the policy of this state that each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees.” The opinion cited Tex. Att’y Gen. ORD-635 (1995) for the proposition that

Records that [are] clearly related to official business are public records subject to the act regardless of whether an individual member of a governmental body, the governmental body’s administrative offices, or the custodian of records holds the records. If a governmental body could withhold records relating to official business simply because they are held by an individual member of the governmental body, it could easily and with impunity circumvent the act merely by placing all records relating to official business in the custody of an individual member. The legislature could not have intended to permit governmental bodies to escape the requirements of the act so easily.

²⁰ Tex. Att’y Gen. ORD-225 (1979) *citing Crabb v. Uvalde Paving Co.*, 23 S.W.2d 300, 302 (Tex. Comm’n App. 1930, holding approved); *Stirman v. City of Tyler*, 443 S.W.2d 354, 358 (Tex. App.—Tyler 1969, writ ref’d n.r.e.); *City of Floydada v. Gilliam*, 111 S.W.2d 761 (Tex. App.—Amarillo 1937, no writ); *Board of School Trustees of Lubbock County v. Woodrow Independent School District*, 90 S.W.2d 333 (Tex. App.—Amarillo 1935, no writ); *Toyah Independent School District v. Pecos-Barstow Independent School District*, 466 S.W.2d 377, 380 (Tex. App.—San Antonio 1971, no writ).

²¹ See Tex. Atty. Gen. OR2001-1790.

Further, the opinion repudiated the argument that the emails were not information connected with "official business" because one city council member's statements cannot constitute an official act binding the city.

The one ray of light in the opinion is fact-based. The City of Arlington councilmember solicited citizens to communicate with her as a councilmember on her personal computer by including the home email address on her city business card. Accordingly, the opinion appeared to rely somewhat on the fact that the councilmember made the decision to solicit city-business transactions over a home computer through her business card.²² According to the City of Arlington, the case is currently being appealed, but no final disposition has been reached.

On a more positive note, the City of Bedford received a similar request for emails in 2001.²³ The city's outside counsel made arguments similar to those of Arlington's attorney, stating that the email in question was created for personal use of the sender (the mayor) and recipients (all city employees), and that it was neither created nor maintained under a law or ordinance or connected to official business of any kind. Concluding that the information at issue was not used in the transaction of official business and was thus not public information under the TPIA, the attorney general did not require the release of the email. The opinion provided a list of criteria to be used in determining whether email is essentially personal in nature or whether it contains information that is collected, assembled, or maintained by or for a governmental body:

- 1) who prepared the document;
- 2) the nature of its contents;
- 3) its purpose or use;
- 4) who possessed it;
- 5) who had access to it;
- 6) whether the employer required its preparation; and
- 7) whether its existence was necessary to or in furtherance of the employer's business.²⁴

While not truly ameliorating the previous conclusion that home email may be subject to the TPIA, the Bedford opinion provides criteria by which a city may argue whether a particular email must be released.²⁵

²² *But see* Tex. Att'y Gen. OR2002-2781 (concluding that request for mayor's home computer address book required mayor to release addresses of those related to town business, but not those of personal contacts).

²³ See Tex. Att'y Gen. Op. OR2001-3828.

²⁴ Tex. Att'y Gen. ORD-635 (1995)(citing *In re Grand Jury Proceedings*, 55 F.3d 1012, 1014 (5th Cir. 1995)).

²⁵ See also Tex. Att'y Gen. OR2001-1434 (concluding that email received by councilmember at his private website does not constitute public information).

In January 2004 letter ruling, the attorney general considered an information request for a journal kept by a mayor in his home. The attorney general stated that:

[I]nformation is public information within the scope of the Act when it relates to the official business of a governmental body or is maintained by a public official or employee in the performance of an individual. See Open Records Decision No. 635 at 4 (1995). Information is not beyond the scope of the Act simply because the information is in the possession of a particular official or employee of a governmental body, rather than the governmental body as a whole. . . . On the contrary, information that clearly relates to a governmental body's official business is subject to the Act, regardless of whether the information is held by a particular official or employee, the governmental body's administrative offices, or the custodian of records.²⁶

Although the information sought in this matter was a journal, rather than email correspondence, the analysis is instructive on the issue of email generated or received on an official or employee's home computer.

At least one subsequent opinion made no argument as to whether home emails should be released.²⁷ However, the city in that case did raise exceptions to disclosure, which the attorney general's office granted. The City of Arlington, in requesting the opinion discussed above, did not raise any exceptions to disclosure. Thus, the lesson to be learned is that, even though a councilmember's home emails may be "public information" as defined by the TPIA, the emails may still be withheld if an exception to disclosure applies.

Exceptions to Disclosure

While email is a relatively new form of information under the TPIA, the same exceptions to disclosure apply to email just as they do to any other document or correspondence. Although a full discussion of all of the myriad exceptions to disclosure found in the TPIA is beyond the scope of this paper, a very brief, non-exhaustive, discussion of some relevant attorney general opinions follows to illustrate the previous statement.

Law Enforcement Exception - OR2001-6125: Texas Education Agency allowed to withhold emails containing information related to a law enforcement investigation under § 552.108.²⁸

²⁶ Tex. Att'y Gen. OR2004-0327 at 2.

²⁷ See Tex. Atty. Gen. Op. OR2001-4625 (request for all emails and electronic faxes related to city business that have been sent or received by Mayor on her home computer... from May of 1999 to the present).

²⁸ *But see* Tex. Atty. Gen. OR2001-2334 for a frightening opinion that requires the release of police emails sent to and from all mobile computer equipped patrol cars. The opinion concluded that the release of the information would not interfere with law enforcement under §552.108.

Attorney Client Privilege - OR2001-4111 and OR2001-4183: city allowed to withhold privileged emails containing communications between the city's attorney and the city which contain client confidences and legal advice or opinions under § 552.107.

Agency Memoranda - OR2001-3457: Texas Parks and Wildlife Department allowed to withhold emails under § 552.111 that constituted interagency and intra-agency memoranda and letters, but only to the extent that they contain advice, opinion, or recommendation intended for use in the policymaking process and not merely facts and written observation of facts and events that are severable from advice, opinions, and recommendation.

These opinions simply serve to illustrate that the exceptions to disclosure in the TPIA apply to email just the same as any other type of public information maintained by a city.

RECORDS RETENTION

Records Retention Schedule

The Local Government Records Act (LGRA) is codified in Chapters 201 through 205 of the Texas Local Government Code. The LGRA provides that, on or before June 1, 1990, the governing body of each local government should have designated a records management officer.²⁹ The LGRA further provides that, by January 1, 1991, the governing body should have established a records management program.³⁰ On or before January 4, 1999, all cities were required to prepare and file with the Director of the Texas State Library and Archives Commission (TSLAC) a records control schedule.

TSLAC has promulgated model records retention schedules. The schedules are available on the Internet at www.tsl.state.tx.us or by calling 512-454-2705. In addition, TSLAC conducts training for local governments around the state.

The current model records retention schedule for local governments promulgated by TSLAC does not address email. However, TSLAC has drafted a sample "Model Policy for Records Management Requirements for Electronic Mail." The policy is available from TSLAC at <http://www.tsl.state.tx.us/slr/recordspubs/lgbullb.html>.

Email No Longer in Existence

The attorney general has issued several opinions regarding email that is no longer in existence. The analyses in these opinions are favorable to cities, but caution should be taken to assure compliance with any applicable records retention policies.

²⁹ Tex. Loc. Gov't Code § 203.025(a).

³⁰ *Id.* at § 203.026(a).

The TPIA applies only to information in existence at the time a request is made.³¹ The TPIA does not require a governmental body to prepare new information in response to a request.³² A governmental body must only make a good faith effort to relate a request to information which it holds.³³ Thus, if a city does not maintain any emails that are responsive to a request, the TPIA does not apply.³⁴

Deleted Email

The attorney general's office has addressed in several opinions whether email in various stages of deletion from a computer hard drive is in existence.

Computer software programs keep track of the location of files by storing the location of data in a file allocation table (FAT) of a computer's hard disk. The software then displays the file as being in a specific storage location. Usually, but not always, when a file is "deleted," it is not actually deleted. Rather, the display of the location is merely shown to be moved to a "trash bin" or "recycle bin." Later, when files are "deleted" or "emptied" from these "trash bins," the data is usually not deleted, but the location of the data is deleted from the FAT. Some software programs immediately delete the location information from the FAT when a file is deleted. Once the location reference is deleted from the FAT, the data may be overwritten and permanently removed. To the extent an email responsive to a request has only been placed in the "trash bin" or "recycle bin" of a program, the email is still being "maintained" by the city for purposes of the TPIA and is still considered "public information." However, to the extent an email responsive to a request has been deleted from the trash bin, and thus the location of the file on the hard drive has been deleted from the FAT, the attorney general has concluded that the email is no longer being "maintained" by the city and is no longer public information.

Therefore, to the extent email responsive to a request are still contained in a trash bin of a city - or possibly home - computer at the time of the request, the city is obliged to retrieve those emails and promptly make them available to the requestor or submit them to the attorney general for a decision.³⁵ In short, if the email is either still on a hard drive because it is in an "in" box or still in the "deleted items" or recycle bin, it is subject to the TPIA.

In one recent case, a hospital district received a request for certain correspondence of an employee. The employee "recalled one or two emails that may have referenced the requestor, but that after searching his emails, found that no such emails existed in his files or computer." The hospital district subsequently notified its information services department in an attempt to recover

³¹ See TEX. GOV'T CODE §§ 552.002, 552.021, 552.227, & 552.351.

³² See Attorney General Opinion H-90 (1973); see also Tex. Atty. Gen. ORD-87 (1975), 342 at 3 (1982), 416 at 5 (1984), 452 at 2-3 (1986), 555 at 1-2 (1990), 572 at 1 (1990).

³³ See Tex. Atty Gen. ORD-561 (1990).

³⁴ See, e.g. Tex. Atty Gen. OR2001-6057.

³⁵ Tex. Atty Gen. OR2001-3366.

any emails that may have been deleted from the employee's computer. Tacitly concluding that the investigation was unnecessary, the attorney general's office concluded that the TPIA compels disclosure of public information that is in existence, but it does not require a government entity to prepare or assemble new information in response to a request.³⁶ While the hospital district appeared to dodge a bullet in that particular scenario, city officials should be aware of the criminal penalties for destroying public information.

Destroying Public Information

Section 202.001 et seq. of the Local Government Code governs destruction of records. According to that section, no record may be destroyed unless it is listed on a records control schedule and the time for retention has expired or the record is exempt from the records control schedule. Further, under Chapter 202 and the TPIA, a record that is the subject of litigation or a public information request may not be destroyed until the litigation is settled or the request is resolved.

Section 552.351 of the TPIA prohibits the destruction, removal, or alteration of public information. A person commits an offense if the person willfully destroys, mutilates, removes without permission, or alters public information. An offense under § 552.351 is a misdemeanor punishable by a fine of not less than \$25 or more than \$4,000, confinement in the county jail for not less than three days or more than three months; or both the fine and confinement.³⁷ Thus, to avoid inadvertently destroying emails that should be retained, a city should amend its records retention schedule to provide guidelines for city officers and employees. In any case, no email that may be responsive to a request should be deleted after a request for the information has been received.

Conclusion and Suggestions

Because there is so little law on the topic of email and the TPIA, this section provides some practical tips for dealing with email.

When using email to conduct public business, keep the following tips - originally authored by Alan Bojorquez³⁸ - in mind:

1. Evaluate the sensitivity of the communication and the potential costs of inadvertent disclosure.
2. Don't say anything in an email that you would not print on letterhead and sign your name to.
3. Be descriptive in the "subject" line.
4. Try to limit the message to a single subject.

³⁶ Tex. Att'y Gen. OR2001-3199.

³⁷ See also TEX. LOC. GOV'T CODE § 202.008 (Class A misdemeanor to destroy a record listed in records retention schedule).

³⁸ These tips were authored by Alan J. Bojorquez, a founding partner in the law firm of Bovey, Akers, & Bojorquez in Austin.

5. Use caution when instinctively replying to a message you have received.
6. Avoid airing disputes over email.
7. Be selective when copying or blind copying other recipients on a message.
8. Be deliberate when forwarding emails.
9. Protect privileged or confidential information.
10. Diligently maintain your files and clean your system regularly.
11. Understand that employers can inspect employee email in certain situations.
12. Remember that if you want to withhold an email that is responsive to an public information request, you must submit the document to the attorney general to determine if it is privileged, confidential, or subject to an exception.

Further, city officers and employees should be made aware that emails regarding city business may be subject to disclosure and records retention policies of the city, even if the email is sent to or from a computer away from city hall. Sample guidelines are included as an appendix to this paper.

In addition, any entity that is subject to the TPIA should develop a policy governing how public information requests are dealt with. The policy should designate who handles requests, where facsimile or email requests should be sent, are requests required to be in writing, and when should legal counsel be consulted regarding a request.

OPEN MEETINGS ACT

Introduction

The Texas Public Information Act is not the only open government law that is implicated by the use of email. Email also merits caution under the Texas Open Meetings Act (TOMA). The TOMA provides that meetings of governmental bodies must be open to the public, except for expressly authorized executive sessions, and that the public must be given notice of the time, place, and subject matter of meetings of governmental bodies.³⁹

The political theory behind the TOMA is that, in a representative form of democracy, city councils and other governmental bodies govern with the consent of their constituents. Thus, the citizens who elected their leaders have the right to observe their government in action, including not only the voting record of their elected representatives, but also the deliberations by which those decisions are made.

While there are no Texas cases or attorney general opinions that deal specifically with deliberations through email, the reasoning of decisions in other jurisdictions

³⁹ TEX. GOV'T CODE Chapter 551.

and decisions and opinions on other Texas topics may be extrapolated and applied to provide some guidance in the area. More important to Texas is the fact that the TOMA has been construed to apply to situations in which members of a governmental body act as a body but are not in each other's physical presence.

Other Jurisdictions

In 2001, a Washington appeals court held that a series of emails between members of a school board constituted a meeting. In *Wood v. Battle Ground School District*, four out of five school board members sent each other email messages discussing whether a school district employee should be terminated.⁴⁰ When the employee was later fired, she sued the school district for violations of Washington's Open Public Meetings Act.

The appeals court held that the exchange of emails can constitute a meeting if members communicate about issues that may or will come before the board for a vote. In doing so, however, the court recognized the need for balance between the right of the public to have its business conducted in the open, and the need for members of governing bodies to obtain information and communicate in order to function effectively. The opinion emphasized the fact that the mere use or passive receipt of email does not automatically constitute a meeting.⁴¹

According to the Washington court, the employee established a prima facie case of "meeting" by emails. The email discussions involved a quorum of the five-member school board, and the discussions related to board business (including the possibility of instituting a declaratory judgment in regard to an employee's contract with the school district and otherwise evaluating the employee's performance). "[T]he active exchange of information and opinions in these e-mails, as opposed to the mere passive receipt of information, suggests a collective intent to deliberate and/or to discuss Board business."

As the Florida Supreme Court stated more than thirty years ago:

During past years tendencies toward secrecy in public affairs have been the subject of extensive criticism. Terms such as...secret meetings, closed records, [and] executive sessions...have become synonymous with 'hanky panky' in the minds of public-spirited citizens. One purpose of the Sunshine Law was to maintain the faith of the public in governmental agencies. Regardless of their good intentions, these specified boards and commissions, through devious ways, should not be allowed to deprive the public of this

⁴⁰ 27 P.3d 1208 (2001).

⁴¹ *Id.* ("The OPMA is not implicated when members receive information about upcoming issues or communicate amongst themselves about matters unrelated to the governing body's business via e-mail.")

inalienable right to be present and to be heard at all deliberations wherein decisions affecting the public are being made.⁴²

This type of rhetoric seems to prevail throughout the judicial system. Words like “devious” and “secret” are often used in the newspapers and court opinions. In reality, most local government officials are merely trying to serve their constituents to the best of their ability.

In Canada, the Ontario Court of Appeals ruled that the term “‘meeting’ should be interpreted as a gathering to which all members of [a governing body] are invited to discuss matters within their jurisdiction.”⁴³ The court further held that all councilmembers do not have to be physically present in order for a meeting to be held and that the key question is whether “*matters which would ordinarily form the basis of Council’s business are dealt with in such a way as to move them materially along the way in the spectrum of an overall council decision.*”

The previous quote appears to be indicative of the direction courts and attorney generals throughout Canada and the United States are taking. When in doubt, any discussion - be at in person, on the telephone, or by email - between a quorum of members of a governmental body, at which public business is discussed, is subject to open meetings law.

Telephone Conversations, Letters, and Email

While no Texas law specifically addresses deliberation by email, the law governing deliberations by telephone or letter is instructive.

The TOMA requires a governmental body to meet in properly noticed public meetings unless the governmental body is expressly authorized by law to discuss an item in closed session.⁴⁴ The TOMA defines a meeting as “a deliberation between a quorum of a governmental body, or between a quorum of a governmental body and another person, during which public business or public policy over which the governmental body has supervision or control is discussed or considered or during which the governmental body takes formal action.”⁴⁵

“Deliberation” means “a verbal exchange during a meeting between a quorum of a governmental body, or between a quorum of a governmental body and another

⁴² *Id.* at footnote 3, citing *Bd. of Pub. Instruction v. Doran*, 224 So.2d 693, 699 (Fla. 1969).

⁴³ See “*Local Government Luddites and E-meetings in Canada*,” *Municipal Lawyer Magazine*, IMLA, January/February 2002, Vol. 43, No. 1.

⁴⁴ See TEX. GOV'T CODE §§ 551.002 (“Every regular, special, or called meeting of a governmental body shall be open to the public, except as provided by this chapter.”), 551.041 (notice), 551.071-551.086 (exceptions to requirement that meetings be open).

⁴⁵ *Id.* at § 551.001(4)(A); See also *Id.* at § 551.001(4)(B)(alternate definition of a meeting); § 551.001(4)(B)(iv)(“The term does not include the gathering of a quorum of a governmental body at a social function unrelated to the public business that is conducted by the body, or the attendance by a quorum of a governmental body at a regional, state, or national convention or workshop, if formal action is not taken and any discussion of public business is incidental to the social function, convention, or workshop.”).

person, concerning an issue within the jurisdiction of the governmental body or any public business."⁴⁶ "Verbal exchange" does not mean only spoken communication. Under the attorney general's interpretation, the term also applies to written communications and email.⁴⁷

The TOMA contains two criminal misdemeanor provisions that are potentially relevant to the use of email. Each of these offenses is punishable by a fine of not less than \$100 or more than \$500, confinement in the county jail for not less than one month or more than six months, or both fine and confinement.

Section 551.143 provides that:

(a) A member or group of members of a governmental body commits an offense if the member or group of members knowingly conspires to circumvent this chapter by meeting in numbers less than a quorum for the purpose of secret deliberations in violation of this chapter.

Section 551.144 provides that:

(a) A member of a governmental body commits an offense if a closed meeting is not permitted under this chapter and the member knowingly:

(1) calls or aids in calling or organizing the closed meeting, whether it is a special or called closed meeting;

(2) closes or aids in closing the meeting to the public, if it is a regular meeting; or

(3) participates in the closed meeting, whether it is a regular, special, or called meeting.⁴⁸

A member of a governmental body may be "held criminally responsible [under section 551.144] for his involvement in the holding of a closed meeting which is not permitted under the TOMA regardless of his mental state with respect to whether the closed meeting is permitted under the Act."⁴⁹ However, it is a

⁴⁶ *Id.* at § 551.001(2).

⁴⁷ Op. Tex. Att'y Gen No. JC-0307 (2000)(concluding that the TOMA's definition of "deliberation" does not exclude all forms of nonspoken exchange, such as written materials or electronic mail) (Also concluding that if only spoken communications are included in the definition of "deliberation," members of a governmental body could easily avoid the TOMA's requirements by discussing public business via written notes and electronic mail and declining to give the term "deliberation" such a limited construction).

⁴⁸ See also TEX. GOV'T CODE at § 551.001(1) ("Closed meeting' means a meeting to which the public does not have access.").

⁴⁹ *Tovar v. State*, 978 S.W.2d 584, 587 (Tex. Crim. App. 1998)(en banc).

defense to prosecution under section 551.144 "that the member of the governmental body acted in reasonable reliance on a court order or a written interpretation of this chapter contained in an opinion of a court of record, the attorney general, or the attorney for the governmental body."⁵⁰

Based on all of the statutory provisions above, the attorney general has concluded that members of a governmental body may violate the TOMA by signing a letter on matters relevant to public business without meeting to take action on the matter in a properly posted and conducted open meeting.⁵¹ The San Antonio Court of Appeals also reached this same conclusion.⁵² The court held that members of a school board violated the TOMA by deciding to send out a letter to all parents of the school district without discussion of the matter in an open meeting. The physical presence of a quorum in a single place at the same time is not always necessary for a violation to occur.⁵³ Similarly, the circulation of any document that requires approval of the governing body to take effect in lieu of its consideration at a meeting would violate the TOMA.⁵⁴

In an unpublished opinion, the United States District Court examined whether the San Antonio City Council had violated the Open Meetings Act by meeting in person and by telephone in groups of less than a quorum to discuss city budget the night before a scheduled Council meeting. Members were brought in and out of the discussion in order to avoid the physical gathering of a quorum. Court found that the arrangement had created a "walking forum" and that in fact a quorum of the Council had deliberated and reached an agreement on the budget. Court concluded Open Meetings Act had been violated.⁵⁵ This case includes a lengthy discussion about open meetings laws in Texas and in other jurisdictions.

Analogizing the above analysis to email, the attorney general or a court would likely hold that - similar to the Washington email case - a governing body that comes to some decision on public business or policy through exchanged emails would violate § 551.144 of the TOMA by participating in a "meeting" that is not open to the public. For example, suppose a city staff member sent an email to one councilmember and copied all of the councilmembers. This action by itself should not constitute a violation. However, if the councilmembers responded to

⁵⁰ TEX. GOV'T CODE § 551.144(c).

⁵¹ Tex. Att'y Gen. Op. No. DM-95 (1992); See also Tex. Att'y Gen. Op. No. LO-95-055 ("It is possible for members of a governmental body to violate the Open Meetings Act even [though] they are not physically present in one place, for example, by discussing public business of the governmental body over the telephone.").

⁵² See *Hitt v. Mabry*, 687 S.W.2d 791 (Tex. App.-San Antonio 1985, no writ).

⁵³ *But see Harris County Emergency Serv. Dist. No. 1 v. Harris County Emergency Corps*, 999 S.W.2d 163, 169 (Tex. App.-Houston [14th Dist.] 1999, no pet.)(finding, absent evidence of secret deliberations attempting to circumvent the Act, that where less than a quorum of a governmental body meets together they have not had a "meeting" for purposes of the Act and have not violated the Act).

⁵⁴ Op. Tex. Att'y Gen. No. JC-0307 (2000).

⁵⁵ *Esperanza Peace and Justice Center v. City of San Antonio*, 2001 U.S. Dist. Lexis 6259.

the staff member or a quorum of the other councilmembers as to what action to take in response to the original email, a violation may have occurred. Thus, caution is warranted.

The mere fact that two councilmembers visit over the phone does not in itself constitute a violation of state law. However, if city councilmembers are using individual telephone conversations to poll the members of the council on an issue or are making such telephone calls to conduct their deliberations about public business, there may be the potential for criminal prosecution. Physical presence in one place is not necessary to violate the Open Meetings Act.⁵⁶ Whether phone conversations between less than a quorum of a city council is a violation of the TOMA is a fact question.⁵⁷ Such interactions could amount to meeting in numbers less than a quorum to circumvent the purposes of the Open Meetings Act. Similarly, if two members of a governing body meet in numbers less than a quorum by deliberating through email, a violation of § 551.143 may occur.

Agenda Setting

Nothing prohibits an individual citizen or employee who is not a member of the governing body from urging individual members of a governing body to place an item on an agenda or vote a certain way on an item on the agenda, whether through email or other means.

Further, the attorney general has concluded that an individual member of a governing body does not violate the TOMA when he or she communicates in writing to a staff member indicating a desire to have an item placed on the agenda and sends a copy to other members of the board.⁵⁸

Procedures related to agenda preparation should not involve deliberations among a quorum of members of a governmental body outside of a properly-posted public meeting.⁵⁹

Aiding and Abetting

A person who is not a member of a governmental body may be criminally liable under the TOMA. Sections 551.143 and 551.144 appear to only apply to members of a governmental body. However, the Texas Penal Code applies to the TOMA's criminal provisions.⁶⁰ Under Chapter 7 of the Penal Code, a person

⁵⁶ Op. Tex. Att'y Gen. No. DM-95 (1992).

⁵⁷ *Hitt v. Mabry*, 687 S.W.2d 791 (Tex. App. – San Antonio 1985, no writ)(school trustees violated Open Meetings Act by telephone conferencing); and *Harris County Emergency Service Dist. #1 v. Harris County Emergency Corps*, 999 S.W.2d 163 (Tex. App – Houston [14th Dist.] 1999, no writ.) (holding that evidence that one board member of five-member county emergency service district occasionally used telephone to discuss agenda for future meetings with one other board member did not amount to Open Meetings Act violation).

⁵⁸ Op. Tex. Att'y Gen. MW-432 (1979).

⁵⁹ Op. Tex. Att'y Gen. DM-473 (1998).

⁶⁰ See *Martinez v. State*, 879 S.W.2d 54, 56 n.4 (Tex. Crim. App. 1994) (en banc) (concluding that Penal Code applies to Open Meetings Act offenses); Tex. Pen. Code § 1.03(b)(Penal Code

who intentionally aids a public officer in the commission of an offense that may only be committed by a public officer may be charged as if he or she had directly committed the offense.⁶¹ Thus, the law permits the charging of a person who is not a member of a governmental body with an offense under the TOMA.

Keep in mind that a person who approaches the members of a governing body on his or her own initiative and not upon the request of other members of the governing body, and does not act in concert with a member or members of the governing body, does not violate the TOMA. The attorney general's position on aiding and abetting should not impede citizens' access to public officials elected to represent their interests or penalize public officers for being open to their constituents because a nonmember may not be criminally liable under the TOMA unless, acting with intent, he or she aids or assists a member or members of the governmental body who knowingly act to violate the TOMA.⁶²

Conclusion and Suggestions

Email, by its very nature, creates a tremendous potential and temptation for substantive discussions without the public's knowledge or opportunity to observe. What makes email so potentially troublesome is that it has the informality of a telephone. However, unlike talking on the telephone, it is much easier to create a "conference" among a significant portion of the city council simply by creating an electronic councilmember distribution list. Because email creates a verbatim recording of an entire series of communications, it can provide "smoking gun" evidence of open meetings violations. Council members should, therefore, treat email as if it were a recorded and transcribed telephone call.

Council members should also be aware that the TOMA also applies to communications of less than a quorum of the city council in certain circumstances. Thus, councilmembers should also avoid intentionally deliberating in groups of less than a quorum, by email or otherwise, for the purpose of circumventing the TOMA.

SEXUAL HARRASSMENT

Along with the substantial benefits that email brings to the workplace, numerous problems and unintended effects are also starting to emerge. The technology of email fosters a heightened sense of psychological distance between communicators and a greater perception of anonymity. Those two traits often encourage offensive messages, including those that culminate in sexual harassment.

applies to "offenses defined by other laws, unless the statute defining the offense provides otherwise").

⁶¹ See e.g., *Wooley v. State*, 629 S.W.2d 867 (Tex. App. - Austin 1982, pet. ref'd).

⁶² Op. Tex. Att'y Gen. No. JC-0307 (2000).

A full discussion of sexual harassment is beyond the scope of this paper. This section provides a brief introduction to the topic as it relates to email. Very generally speaking, there are two types of sexual harassment: 1) quid pro quo, and 2) hostile work environment.

“Quid pro quo” literally translates to “this for that.” Quid pro quo sexual harassment is implicated when an employee’s submission to unwelcome sexual advances, requests for sexual favors, or other verbal or physical conduct is made an express or implied condition of receiving a job benefit. Quid pro quo sexual harassment is also implicated when an employee’s rejection of unwelcome sexual advances, requests for sexual favors, or other verbal or physical conduct results in a tangible job detriment. A tangible job detriment is a significant change in employment status, such as hiring, firing, failing to promote, reassignment to different responsibilities, or a decision causing significant change in benefits.

A supervisor or other employee may certainly use email as a tool of quid pro quo sexual harassment. However, a more likely scenario involves the use of email to create a hostile work environment.

A hostile work environment is characterized by an employment environment so filled with unwelcome sexual innuendo, remarks, or physical acts as to alter the conditions of the employee’s employment and create an abusive work environment. Examples may include provocative pictures, sexually explicit comments and jokes, comments about body parts, unwelcome touching, and/or other generally unprofessional conduct targeted at one sex or on another. Based on these examples and the frequently sexual content of emails, it is easy to see why email can contribute to a hostile work environment.

Cities should have a strong policy in place to protect both the city and its employees from sexual harassment in any form, including email.

ATTORNEY-CLIENT RELATIONSHIP

The use of email raises two issues with respect to legal advice: (1) the lawyer’s duty of confidentiality, and (2) the lawyer-client privilege.

Confidentiality

The Texas Disciplinary Rules of Professional Conduct govern a lawyer’s behavior with respect to his or her client. Under the rules, a lawyer may not generally reveal confidential information given by a client to anyone other than the client or the client’s representatives.⁶³

⁶³ TEX. DISCIPLINARY R. PROF’L CONDUCT 1.05.

The duty of confidentiality is implicated by a lawyer's use of email to transmit confidential information. An email message sent via the internet is broadcast in plain text to an unpredictable number of hosts in an unpredictable fashion. Each email may go through a number of different computers on the way to its destination. Each of these computers keeps a copy of the email for some amount of time. Thus, anyone with access, legal or illegal, to the "stopover" computer system could read the email.

Aside from encryption, most lawyers simply attach a disclaimer to the bottom of each confidential email, such as:

The contents of this message may be confidential and subject to the attorney/client privilege. If you are not the intended recipient(s) of this message, please destroy this message immediately. No permission is given for persons other than the intended recipient(s) to read or disclose the contents of this message.

The American Bar Association approved this method as sufficient to protect confidential information transmitted via email, so long as the lawyer has consulted with his or her client as to the acceptability of transmitting information in this manner.⁶⁴

Lawyer-Client Privilege

"A client has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client."⁶⁵ The lawyer-client privilege, as spelled out in the Texas Rules of Evidence, is less broad than the lawyer's duty of confidentiality. Whereas the lawyer's duty of confidentiality generally prohibits disclosure of client information at any time, the purpose of the lawyer-client privilege is to secure the free flow of information between attorney and client on legal matters without the fear that details of their communication will be required to be disclosed in a court proceeding.⁶⁶

For the privilege to apply, (1) the holder must be (or have sought to become) a client, (2) the person to whom the communication was made must be an attorney acting as such at the time, (3) the communications must be made in confidence, and (4) the communications must be made for the purpose of receiving legal assistance.⁶⁷

⁶⁴ American Bar Association Formal Ethics Opinion 99-413 (1999).

⁶⁵ TEX. R. EVID. 503(b).

⁶⁶ *Ford Motor Co. v. Leggat*, 904 S.W.2d 643, 647 (Tex.1995).

⁶⁷ TEX. R. EVID. 503; Effective March 1, 1998, Rule of Evidence 503 was amended to adopt the "subject matter" test for an entity's assertion of the privilege, replacing the "control group" test previously used. *National Tank Co. v. Brotherton*, 851 S.W.2d 193, 197-98 (Tex. 1993). Under the subject-matter test, an employee's communication is deemed to be that of the corporation/client if the employee makes the communication at the direction of his superiors in the corporation and where the subject matter upon which the attorney's advice is sought by the

The client holds the privilege, and can waive it intentionally or inadvertently. If the client intentionally discloses “confidential” information to an outside third party, the privilege is waived. Inadvertent disclosure is a more difficult problem, and is determined on a case-by-case basis, taking into account the circumstances surrounding the disclosure. The most important factor to be considered is whether reasonable precautions were taken to protect the information.⁶⁸ For this reason, confidential email messages to and from clients should bear a notation strongly asserting the lawyer-client privilege. Forwarding of email communications from legal counsel should be strictly prohibited. Also, confidential communications between clients and legal counsel should be saved by the sender and recipient, but should be kept separate from documents that are required to be disclosed to the public.

In any case, a city should develop a policy that specifically addresses preservation of the lawyer-client privilege, and further protection of confidential communications should be considered according to the content of communications.

PRIVACY ISSUES

Introduction

Privacy as it relates to email in the government workplace in Texas is an oxymoron. By definition, any document that relates to city-business, paper or electronic, that is produced or received by a city official or employee is public information. Because of this, “privacy” as it relates to email generally involves personal email sent or received on city equipment. The following sections deal with an employee’s right to privacy on his or her work computer.

In any case, there is no such thing as a truly private email. Internet email is far from secure from a dogged hacker, and with most email systems the email administrator has the ability to read all email messages, even those that have been deleted.

The general rule with email should be not to send anything by email that you would not want anyone and everyone in the world to see. If you are debating whether or not to send something by email, either deliver it by hand or send it by regular mail. Even items that are originally sent as jokes may be taken out of context and raise serious liability issues.

corporation and dealt with in the communication is the performance by the employee of the duties of his employment. *National Tank*, 851 S.W.2d at 198 (quoting *Harper & Row Publishers, Inc. v. Decker*, 423 F.2d 487, 491-92 (7th Cir.1970), *aff'd per curiam by an equally divided court*, 400 U.S. 348, 91 S.Ct. 479, 27 L.Ed.2d 433 (1971)).

⁶⁸ Some of this material is taken from <http://www.computerbar.org/netethics/bjones.htm>; See also *Allred v. City of Grenada*, 988 F.2d, 1425, 1435 (5th Cir. 1993).

Fourth Amendment

Searches and seizures by government employers or supervisors of the private property of their employees are subject to the restraints of the Fourth Amendment to the United States Constitution, which protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."⁶⁹

However, Fourth Amendment rights are implicated only if the conduct of the government employer violates a reasonable expectation of privacy, and the degree of privacy protection is based on the "operational realities" of the workplace.⁷⁰ By that standard, the question of when a search is "reasonable" depends on the context of a particular employment relationship and the employer's legitimate need to supervise the workplace.⁷¹

Public employer intrusions on the constitutionally protected privacy interests of government employees for work-related purposes, as well as for investigations of work-related misconduct, are judged by the standard of reasonableness under all the circumstances. Thus, if a public employer adopts a policy that states that a public employee's emails are the property of the employer and subject to search or monitoring, and the employee acknowledges the policy, a Fourth Amendment claim by the employee should not succeed because the employee had notice that his or her emails were not private. The receipt of the policy usually serves to eliminate the employee's reasonable expectation of privacy. To this end, an email policy should state that the policy is necessary to protect the public employer's property and maintain an efficient work environment.

Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986 (ECPA) updated older wiretapping statutes by extending privacy protection to communication systems based on computer technology.⁷² Under the ECPA, interception of an email message while it is being transmitted or obtaining the content of a stored message is a federal crime.

There are three exceptions to the ECPA's prohibition that allow an employer to access employee email. To begin with, the "consent" exception removes the ECPA's privacy protection if one of the parties to the communication has given prior consent. An employer should obtain express written consent of the

⁶⁹ *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987).

⁷⁰ *Id.* at 717 ("Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.").

⁷¹ *Id.* ("[W]e note that there was no evidence that the [employer] had established any reasonable regulation or policy discouraging employees...from storing personal papers and effects in their desks or file cabinets.").

⁷² 18 U.S.C. § 2510 et seq. (The ECPA is currently undergoing massive amendments in response to the terrorist attacks of September 11, 2001); See also TEX. PENAL CODE Chapter 16 (containing similar prohibitions and exceptions).

employee to avail itself of this exception, but a written email policy is probably sufficient for this purpose.⁷³

Also, as the "owner" of the email system, an employer is allowed to access an employee's email to assure that it is being used properly by employees (the "business use" exception) and that the technical performance of the system is adequate ("system provider" exception).⁷⁴

Invasion of Privacy

Excessive invasions of privacy, either because the physical space being observed is universally considered to be private (e.g., bathrooms) or because the employer uses its right of access to obtain non-work-related information, should be avoided. For example, if an employer who is monitoring to assure compliance with a policy that prohibits personal use of computer equipment finds an email by a worker that is clearly personal, and the employer reads the entire contents of the email, the act of reading the whole document is more intrusive than simply examining the letter long enough to determine that it is private. An employer who discloses the contents of a personal message to other parties run a risk of liability for invasion of privacy.

While there are several variations on the tort of invasion of privacy, the three elements that must generally be established for an invasion of privacy claim are: (1) an intentional intrusion; (2) upon the seclusion, solitude, or private affairs of another; (3) which would be highly offensive to a reasonable person.⁷⁵

Texas courts require that the intrusion be unreasonable, unjustified, or unwarranted.⁷⁶ Thus, an employee's claim will not usually succeed when an employer has a reasonable, justifiable, purpose for examining email. A written policy stating that email is the property of the employer and that the employee has no privacy right in email on a city computer further strengthens the employer's position. Generally, so long as an employee is made aware that he or she has no privacy rights in email, a claim for invasion of privacy will not lie.⁷⁷

Even if an employee is not aware that his or her email may be examined by the employer, an employer's need to deter unprofessional and potentially illegal conduct may outweigh any privacy interest.⁷⁸

Conclusion

The previous sections dealing with privacy should be taken in context. This is not necessarily a "big brother" issue. Rather, the issue is more about maintaining

⁷³ 18 U.S.C. § 2511(2)(c).

⁷⁴ 18 U.S.C. § 2511(2)(a)(i); § 2701(c)(1).

⁷⁵ *Valenzuela v. Aquino*, 853 S.W.2d 512, 513 (Tex. 1993).

⁷⁶ *Billings v. Atkinson*, 489 S.W.2d 858, 860 (Tex. 1973); *K-Mart v. Trotti*, 677 S.W.2d 632, 636 (Tex.App.--Houston [1st Dist.] 1984, writ ref'd n.r.e.).

⁷⁷ See e.g., *Price v. City of Terrell*, 2000 WL 1872081 (N.D. Tex. 2000).

⁷⁸ *Smith v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996).

an efficient and lawsuit-free workplace. Further, nothing prohibits an employee from obtaining a private computer and email account to use at home for personal email correspondence.

Some people point to several possible drawbacks to an unnecessarily strict email policy. Autonomy is a strongly held value, and the use of highly restrictive policies in the workplace has a potential cost in terms of its effect on the worker's sense of dignity and personal integrity.

Email communication tends to be more informal and spontaneous than communicating with written memos. This quality can foster more efficient workplace communication and productive collaboration. Although restricting email activity to work-related communication seems reasonable and sensible, such a policy may be difficult to carry out in actual practice. A compromise position might be to allow personal use of E-mail to the extent that it doesn't interfere with an employee's productivity and job performance. Thus, city officials should visit with employees and local counsel to determine the level of restriction that is appropriate.

IV. CONCLUSION

Email is an amazing tool that has made many of our lives easier. As with any form of communication, using proper etiquette and complying with rules of common courtesy and applicable laws is essential to avoiding misunderstandings and/or legal liability.

Email is here to stay, and with a little common sense, self-awareness, and sound legal advice, city officials should continue to use this technology without fear.

V. SAMPLE FORMS AND POLICIES

(See next page)

City of Arlington Email Tips

- Provide orientation for new council members on the potential applicability of the open meetings, public information, and records retention statutes to electronic communications and electronically generated documents.
- If possible, provide a specially designated computer and e-mail address to each council member to be exclusively used for city related business.
- Avoid listing private e-mail addresses on official council member letterhead, stationary, official correspondence, or business cards.
- Program some disclosure language to automatically appear in every council member-generated reply message that advises senders that their e-mail responses may be subject to the public information statute for the locality.
- Caution council members against using e-mail to communicate with other council members on subjects and in situations where the e-mail communications would constitute a deliberation that might be subject to the open meetings statute.
- Discourage the use of e-mail by council members to communicate with groups or the entire membership of the city council through use of a group distribution list or series of e-mails to all or a group of individual council members. Emphasize the flow of e-mail communications channels should be with and through the city staff rather than between council members.
- Conspicuously label confidential attorney-client communications sent to council members. It may be helpful to insert a code such as "[C]" in the subject line in order to more readily identify privileged communications.
- Program some records retention files for council members to electronically file messages sent and received.
- Provide guidelines to council members on which items must be retained for records retention purposes and which items may be deleted (e.g., copies of messages or messages of no substantive or administrative value, depending upon the provisions of the records retention statute for the locality).
- Provide city staff to properly manage (electronically file and dispose of) e-mail communications for council members.
- Caution council members about transmitting information prohibited by public information statutes from disclosure. For example, one state recently prohibited the disclosure of citizen e-mail addresses except under certain circumstances. Texas Government Code, Sections 552.136, 552.137.
- Caution council members that once an e-mail document is created it may continue to exist indefinitely within the memories of various computers. E-mail communications thought to have been "deleted" can usually be retrieved by computer technicians in the event of litigation discovery.

ARLINGTON CITY COUNCIL E-MAIL RETENTION GUIDELINES

1. All e-mail is subject to the Council's **Records Retention Schedule**.
2. All e-mail is also subject to public disclosure under the **Public Information Act** (Open Records Act).
3. E-mails should be treated just like correspondence. The content of the e-mail will determine whether or not the e-mail should be retained and the proper retention period.
4. Usually, e-mails which schedule meetings or transmit copies of documents are routine correspondence under the retention schedule and may be disposed of when no longer of administrative value.
5. If the e-mail contains substantive comments, then it is probably not routine correspondence and must be retained in accordance with the Council's Records Retention Schedule.
6. The staff member or official generating and sending, or forwarding, an e-mail to City of Arlington staff and/or other persons and entities is responsible for retaining the message.
7. The City of Arlington staff member or official receiving an e-mail from someone other than City of Arlington staff or officials is responsible for retaining the message.

Texas State Library and Archives Commission

*Model Policy for Records Management Requirements for Electronic
Mail - DRAFT*

[LOCAL GOVERNMENT]

[DATE]

SECTION 1. INTRODUCTION

This policy applies to e-mail used within the government and e-mail used conjointly with the Internet, and does not supersede any state or federal laws, nor any other government policies regarding confidentiality, information dissemination, or standards of conduct. Generally, e-mail should be used only for legitimate government business; however, brief and occasional e-mail messages of a personal nature may be sent and received if the following conditions are met.

SECTION 2. GENERAL GUIDELINES

Personal use of e-mail is a privilege, not a right. Abuse of the privilege may result in appropriate disciplinary action. Employees need to keep in mind that all e-mail is recorded and stored along with the source and destination. Management has the ability and right to view employees' e-mail. Recorded e-mail messages are the property of the agency and therefore the taxpayers of the State of Texas. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to State records retention. Employees should be aware that when sending an e-mail message of a personal nature, there is always the danger of the employees' words being interpreted as official government policy or opinion. Therefore, when an employee sends a personal e-mail, especially if the content of the e-mail could be interpreted as an official government statement, the employee should use the following disclaimer at the end of the message:

"This e-mail contains the thoughts and opinions of [employee name]
and does not represent official [government name] policy."

[OPTIONAL] If the content of the e-mail contains sensitive or confidential information the employee may use the following message at the end of the message:

"This message contains information which may be confidential and
privileged. Unless you are the addressee (or authorized to receive
for the addressee), you may not use, copy or disclose to anyone the

message or any information contained in the message. If you have received the message in error, please advise the sender by reply e-mail and delete the message."

SECTION 3. RESTRICTIONS [OPTIONAL]

Personal e-mail should not impede the conduct of government business; only incidental amounts of employee time--time periods comparable to reasonable coffee breaks during the day--should be used to attend to personal matters. Racist, sexist, threatening, or otherwise objectionable language is strictly prohibited. E-mail should not be used for any personal monetary interests or gain. Employees should not subscribe to mailing lists or mail services strictly for personal use. Personal e-mail should not cause the government to incur a direct cost in addition to the general overhead of e-mail.

SECTION 4. POLICY

It is the policy of [NAME OF GOVERNMENT] to provide for the efficient, economical and effective management of electronic mail records in accordance with Texas Administrative Code (TAC), Chapter 7, Sections 7.71-7.79 and Local Government Code (LGC), Chapter 205, Sections 205.001-205.009 (*Local Government Bulletin B, Electronic Records Standards and Procedures*). TAC, Chapter 7, Section 7.72(d), provides that the governing body of a local government or designated records management officer must administer a program for the management of records created, received, maintained, used, or stored on electronic media.

The [NAME OF GOVERNMENT] desires to adopt a policy for that purpose and to prescribe guidelines and procedures for the management of electronic mail consistent with the Electronic Records Standards and Procedures and in the interest of cost-effective and efficient recordkeeping, including long-term records retention.

SECTION 5. DEFINITIONS

(1) Electronic mail message-A record created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments which may be transmitted with the message.

(2) Electronic mail receipt data-Information in electronic mail systems regarding the date and time of receipt of a message, and/or acknowledgment of receipt or access by addressee(s).

(3) Electronic mail system-A computer application used to create, receive, retain and transmit messages and other records. Excluded from this definition are file transfer utilities.

(4) Electronic mail transmission data-Information in electronic mail systems regarding the identities of sender and addressee(s), and the date and time messages were sent.

(5) Electronic media-All media capable of being read by a computer including computer hard disks, magnetic tapes, optical disks, or similar machine-readable media.

(6) Electronic record-The information that is maintained in electronic format in a computer for computer processing and the product of computer processing of that information that satisfies the definition of a government record in the Local Government Code, Chapter 201, Section 210.003(8).

(7) Electronic records system-Any information system that produces, manipulates, and stores state records by using a computer.

(8) Mailing list service-An electronic mailing list hosting service (e.g., Listserv) used for discussions and announcements within a specified group of individuals. Subscribers to the service participate by sending information to and receiving information from the list using electronic mail messages.

(9) Records management officer-The person who administers the records management program established in each local government under the Local Government Code, Chapter 203, Section 203.026.

(10) Local government record- Any document, paper, letter, book, map, photograph, sound or video recording, microfilm, magnetic tape, electronic medium or other information recording medium, regardless of physical form or characteristic and regardless of whether public access to it is open or restricted under the laws of the state, created or received by a local government or any of its officers or employees pursuant to law, including an ordinance, or in the transaction of public business. The term does not include:

(A) Extra identical copies of documents created only for convenience of reference of research by officers or employees of the local government;

(B) Note, journals diaries, and similar documents created by an officer or employee of the local government for the officer's or employee's personal convenience;

(C) Blank forms;

(D) Stocks of publications;

(E) Library and museum materials acquired solely for the purposes of reference of display;

(F) Copies of document in any media furnished to members of the public to which they are entitled under Chapter 552, Government Code or other state law;

(G) Any records, correspondence, notes memoranda or documents, other

than a final written agreement described by Section 2009.054(c), Government Code, associated with a state department of institution, local government, special district, or other political subdivision of the state participated as a party, facilitated as an impartial third party, or facilitated as the administrator of a dispute resolution system or organization.

SECTION 6. SCOPE

This policy applies to any electronic mail messages created, received, retained, used, or disposed of using the [NAME OF GOVERNMENT'S] electronic mail system.

SECTION 7. RETENTION REQUIREMENTS

The [NAME OF GOVERNMENT'S] approved Control Schedule or Declaration of Compliance with the *Local Government Records Retention Schedules* provide access to the record series and the retention period for each series. It is the content and function of an e-mail message that determines the retention period for that message. All e-mail sent or received by a government is considered a government record. Therefore, all e-mail messages must be retained or disposed of according to the government's retention requirements. E-mail generally (but not always) falls into two common record series categories. These are:

Local Schedule GR, 1000-26, Correspondence and Internal Memoranda:

(b) Administrative – Correspondence and internal memoranda pertaining to or arising from routine administration or operation of the policies, programs, services, and projects of a local government. Retention: 2 years.

(c) Routine – Correspondence and internal memoranda such as letters of transmittal, requests for publications, internal meeting notice and similar routine matters. Retention: AV (after purpose of record is not longer deemed administratively valuable.)

SECTION 8. USER RESPONSIBILITIES

It is the responsibility of the user of the e-mail system, with guidance and training from the Records Management Officer, to manage e-mail messages according to the government's established retention periods. It is the responsibility of the sender of e-mail messages within the government's e-mail system and recipients of messages from outside the government to retain the messages for the approved retention period. Names of sender, recipient, date/time of the message, as well as any attachments must be retained with the message. Except for listserv mailing services, distribution lists must be able to identify the sender and recipient of the message. User responsibilities may be mitigated by the use of a server level automated classification system.

SECTION 9. MAINTENANCE OF ELECTRONIC MAIL

Records created using an e-mail system may be saved for their approved retention period by one of the following:

- (1) Print message and file in appropriate hard copy file.
- (2) Place in folders and save on personal network drive or C:drive.
- (3) Save to removable disk. 3.5" disks are not recommended for retention periods of more than one year due to the instability of this medium.
- (4) Transfer to an automated records management software application.
- (5) Managed at the server by an automated classification system.

Note: Government may include specific instructions for saving e-mail messages to a hard drive. For example using Microsoft Outlook E-mail Application:

How to create a personal folder for e-mail that resides on the C: Drive (your hard drive).

1. Open Outlook
2. Click on "Tools"
3. Click on "Services"
4. Click on the "Add" button
5. Click the bottom line in the text box that says "Personal Folders"
6. This box allows you to designate the drive and folder you want your e-mail to go to. It will default to the Outlook folder. You might want to direct it instead to a folder you have created. Once you designate the folder (at the top of the text box), then name the file that your e-mails will reside in and click "OK" or "Apply" whichever is listed.
7. Now your personal file should appear on the left-hand column of your outlook screen. You can add subdirectories to this (just like you would with the "inbox"). If you file your e-mail here it avoids server problems and gives you some more leeway in storing your files.

SECTION 10. DISPOSITION OF ELECTRONIC MAIL

The process for the legal disposition of government records (including electronic mail) is subject to the same documentation requirements as any other format or medium. This usually requires management permission and some type of disposition log to adequately document disposition and destruction of electronic records. (Local Governments are not required to keep a disposition/ destruction log but the practice is strongly advised.) Section 7.78 of the *Electronic Records Standards and Procedures* (relating to the Destruction of Electronic Records) states that:

- (a) Electronic records may be destroyed only in accordance with the Local Government Code, Section 202.001
- (b) Each local government must ensure that:
 - (1) Electronic records scheduled for destruction are disposed of in a manner that ensure protection of any confidential information; and

(2) Magnetic storage media previously used for electronic records containing confidential information are not reused if the previously recorded information can be compromised by reuse in anyway.

CITY OF _____ COMPUTER USE POLICY
Sample Only - Consult Local Counsel Prior to Adoption

Table of Contents

Section 1 - Purpose of This Policy

Section 2 - Use of the Internet and Email

Section 3 - Monitoring

Section 4 - Permitted Uses of the Internet

Section 5 - Prohibited Uses of Internet and/or Email

Section 6 - Software Security

Section 7 - Passwords

Section 8 - Public Information Requests

Section 9 - Copyright Restrictions

Section 10 - No City Representation

Section 11 - Equipment Maintenance/Protection

Section 12 - Virus Protection

Section 13 - Use of Screen Savers/Background

Section 14 - Violations of This Policy

Section 15 - Exit from Internet

Section 17 - Employee Separation

Section 18 - Execution of Forms

Exhibit "A" - City of _____ Employee Technology Use Agreement

Exhibit "B" - City of _____ Internet/Online Services Use Request

SECTION 1 - PURPOSE OF THIS POLICY

The purpose of this policy is to establish guidelines for the operation of the City's computer system, including both integrated and non-integrated components, and to provide direction as to the appropriate usage of electronic mail (email) and the Internet provided by the City of _____. This policy is intended to protect the property of the City of _____ and to facilitate an efficient working environment.

This policy applies to all personnel utilizing City equipment, software and technology.

SECTION 2 - USE OF THE INTERNET AND E-MAIL

Only those employees who have been specifically authorized in writing by proper authority to use the Internet for City of _____ business shall be allowed to access the Internet, and the sites that are accessed by those who are authorized shall be limited to those sites that relate to the necessary business of the City of _____.

The Internet and email system hardware is to be exclusively used for the purpose of conducting the business of the City of _____, and is the property of the City of _____.

Therefore, all electronic messages completed, sent, or received on the Internet and email system are, and remain, the sole property of the City of _____.

The use of email is public, and is a privilege which is subject to revocation at any time for use that is in conflict with any provision of this policy. Restrictions may be placed upon email use to protect the City and its resources.

Email is not considered private. Therefore employees should not transmit confidential information with this system. Any messages may be utilized in litigation and disciplinary proceedings.

SECTION 3 - MONITORING

The City reserves the right to access and disclose all messages created, sent, and received through its electronic mail system. All electronic messages are retrievable and may be inspected by the City Manager or any other City staff member designated by the City Manager.

The City reserves the right to utilize Internet Surveillance Programs which traces users' steps and monitors employee use of the email system or the Internet. Employees should not consider their Internet usage or email communications to be private.

SECTION 4 - PERMITTED USES OF THE INTERNET

The following are given as examples of permitted uses of the Internet:

- I. Research/Education related to City-related business, communication with professional associations and other governmental entities, universities, businesses and/or individuals associated with the facilitation of City business.
2. Filing of reports relating to various areas of City operations that are required or permitted by state and federal agencies.
3. Distribution of information to the general public under City guidelines and policies for the release of information pursuant to the Texas Public Information Act and other applicable laws.
4. Communication among City employees and professional colleagues, which facilitates work assignments and professional discussion in a work-related field of knowledge.
5. Purchasing, communication with vendors and suppliers, and receiving quotes and obtaining specifications for equipment/material.
6. Registration for conferences, schools and seminars.
7. Making arrangements (airline, hotel, etc.) for travel on City business.
8. Obtaining weather reports.
9. Researching/obtaining news reports from newspapers, publications and other media sources.
10. Receipt of newsletters, bulletins, reports, etc. from professional organizations.
- II. Announcements of personnel vacancies.
12. Any other use that is related to the City's business that is not prohibited by copyright or any other provision of this policy, or any other City policy or state or federal law.

SECTION 5 - PROHIBITED USES OF INTERNET AND EMAIL

- I. Use of the Internet or email system for personal or commercial ventures, religious or political causes, outside organization, or other non job-related matter.
2. Use of the system to create any offensive or disruptive messages. Among those are messages that are unlawful, defamatory, libelous, pornographic, profane, threatening, obscene, harassing, offensive or unprofessional, or that are disrespectful of others, or those that contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses

someone's age, sexual orientation, race, physical attributes, religious or political beliefs, national origin or disability.

3. Accessing any site that is sexually or racially offensive or discriminatory, displaying or downloading or distributing any sexually explicit material, or violation of the City's confidentiality policy.
4. Buying, ordering or bidding on any item that is not properly authorized by proper authority for purchase by the City.
5. Playing games on City of _____ computers is prohibited, except in the case where the employee is on standby duty with no other job function being required at that time, and is specifically authorized to do so by the department head.
6. Gaining, or attempting to gain, unauthorized access to the City's proprietary network or computer system or any other proprietary network or computer system.
7. Any attempt to obstruct other employee's work by consuming gratuitously large amounts of system resources or by deliberately crashing any City computer system.
8. Any attempt to damage computer equipment or software.
9. Any attempt to alter software configurations.
10. Any attempt to cause degradation of system performance.
11. Any use of any City workstation for illegal or criminal purpose.
12. Any violation of copyright laws of software licensing agreements.
13. Downloading or installation of any unauthorized software.
14. Participation in chat rooms.
15. Sending or receiving anonymous e-mail, encrypted messages, or chain letters.
16. Messages shall not be transmitted using another person's name or under an assumed name.
17. Unless specifically authorized to do so by proper authority, employees may not retrieve or read any Internet or email messages for which they are not the intended and appropriate recipient.

SECTION 6 - SOFTWARE SECURITY

All software contained on CD's or disks that are provided with computers and related equipment that is purchased by the City, or those that are directly purchased by the City, are to be kept in a secure location by the appropriate department head, and are not to be used or loaned in any manner that is not consistent with the copyright provisions that apply.

SECTION 7 - PASSWORDS

Personal passwords are not an assurance of confidentiality, and the Internet itself is not secure. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read the message.

Passwords do not belong to the user, as they are the property of the City of _____ and are utilized to protect against non-authorized persons accessing the network system. Employees must disclose all passwords to the designated authority within the City of _____ or they are invalid and cannot be used.

If a user needs to access a different computer than the one that is usually used, the user shall log in using his/her own password.

Users shall not share their password with anyone else other than upon the direction of the City Manager or other City staff member designated by the City Manager.

Users shall not allow other persons to perform any activity with their password. Users are responsible for all activity performed with their password regardless of how it was obtained.

SECTION 8- PUBLIC INFORMATION REQUESTS

All requests for information contained on City computer hard drives or discs that emanate from sources external to the City shall be handled pursuant to the State of Texas Public Information Act as defined in the City's policy for the release of public information.

SECTION 9- COPYRIGHT RESTRICTIONS

The unauthorized reproduction or distribution of copyrighted materials, except as permitted by the principles of "fair use", is prohibited by U. S. copyright law (Title 17, U. S. Code). Any software or other material downloaded (received) or uploaded (sent) by City of _____ computers may be used only with the explicit permission of the copyright holder.

Prior written authorization from the appropriate department head is required before introducing any software into the City of _____ computer system.

Employees may not download entertainment software, games or any other software unrelated to their work.

Any responsibility for any consequences of copyright infringement lies with the user. The City expressly disclaims any liability or responsibility arising from access to or use of information obtained through its electronic information systems, or any consequences thereof.

Unlawful activities will be dealt with in a serious and appropriate manner, and the user may be subject to prosecution by local, state or federal officials. Additionally, disciplinary action, up to and including termination, could be applied.

SECTION 10 - NO CITY REPRESENTATION

Only authorized employees may communicate on the Internet on behalf of the City of _____.

Employees may not express opinions or personal views that could be construed as being those of the City of _____.

Employees may not state their City affiliation on the Internet unless required as part of their assigned duties.

SECTION 11 - EQUIPMENT MAINTENANCE/PROTECTION

Computers are to be cleaned only with compressed air or a moist, lint free rag. Water or cleaning fluid is not to be used on the keyboard, monitor or printer.

Should any computer equipment get wet, the machine is to be turned off and disconnected from the power source. The equipment is not to be turned on again until it has been confirmed that the equipment is moisture free.

In the event of a power outage, the computer and printer are to be disconnected from the power source, and are not to be reconnected until the power source returns to normal.

All computer equipment is to be plugged into an approved surge protector, and never is to be connected directly to the power source.

Repairs and/or modifications to equipment are to be performed only by qualified technicians designated by the appropriate City authority .

SECTION 12 - VIRUS PROTECTION

All City of _____ computers are to be equipped with up-to-date virus protection software, and all external software that is introduced into City computers is to be checked for viruses before use in the system.

Users shall leave the virus protection software enabled at all times. Anti-virus software is to be kept current by ensuring that updated revisions are downloaded at such intervals as are recommended by the vendor.

It should be noted that the virus detection software will detect viruses, but will not automatically eliminate them. Therefore, the user must follow the prompts from the virus protection software.

Emails that do not clearly identify the sender are not to be opened. E-mails from senders that you do not recognize are not to be opened.

Email attachments that are executed files, with an .EXE or .COM extension, are not to be opened without first scanning them with a virus checker and confirming their legitimacy.

SECTION 13 - USE OF SCREEN SAVERS/BACKGROUNDS

No screen savers or background are to be used on any City of _____ computer that is deemed to be offensive or inappropriate by the responsible department head.

SECTION 14 - VIOLATIONS OF THIS POLICY

Any violation of this policy or use of the Internet or email for improper purposes shall subject the employee to loss of computer access and/or disciplinary action, including immediate termination.

SECTION 15 - EXIT FROM INTERNET

When not actively utilizing Internet service, users shall terminate the Internet connection.

SECTION 16 - EMPLOYEE SEPARATION

Upon separation from the City's employment, the former employee's access to the City's computer system and all of its components shall be immediately revoked.

SECTION 17 - EXECUTION OF FORMS

Exhibit "A" - Employee Agreement Form: This form confirms that the user employee will read, understand, and comply with all of the provisions of this policy. All employees whose job duties require or allow use of the City's technology shall be required to sign this form after they have read the policy.

Exhibit "B" - Internet/Online Services Use Request Form: Execution and approval of this form is required for all employees whose job duties require or allow the use of Internet/Online Services.

Exhibit " A " - City of _____ Employee Technology Use Agreement:

I have read and I understand all of the terms and conditions enumerated in the City of _____ Computer Use Policy, and I agree to fully abide by all provisions of this policy, and as may hereafter be amended.

Employee Signature

Department

Date