City of Pembroke Pines

PEMBROKE PINES All-America City 2004

INTER-OFFICE CORRESPONDENCE

MEMORANDUM NO. 2007-245

TO: Aurora Gonzalez, Human Resources Administrator

CC: Charles F. Dodge, City Manager
Chief Dan Giustino, Pembroke Pines Police Department
Dave Frank, Administrative Services Director

FROM: Samuel S. Goren, City Attorney SSG
David N. Tolces, Assistant City Attorney DNT

DATE: October 4, 2007

RE: City of Pembroke Pines ("City") / General Policy on the Use of Computers and Data Communications

Pursuant to your request, we have revised the City of Pembroke Pines General Policy on the Use of Computers and Data Communications.

Attached is a copy of the revised General Use of Computers and Data Communication, as well as Internet Policies and Guidelines for the City's policy on the Information Systems. The revisions are contained in the second paragraph of Section I of the Internet Policies and Guidelines, and in Section III, "Employees Internet Usage Policy". In light of the change to these policies, it **will** be necessary for the City to have each employee sign a new document verifying that they received the revised policy. If you would like assistance with the preparation of the form, we will be happy to assist.

If you have any other questions or concerns, please do not hesitate to contact our office.

Enclosure(s)
SSG:DNT:js
H:\760185.PP\MEMO 2007\2007-245 (Computer policy).doc

City of Pembroke Pines
General Policy on the Use of Computers and Data Communications

I. PURPOSE

The City of Pembroke Pines provides computer access and capabilities through Information Technology Services. The City of Pembroke Pines relies heavily upon these systems to meet operational, financial, and informational needs. It is essential that the City's computer systems, and computer networks, as well as the date they store and process be operated and maintained in a secure environment and in a responsible manner. It is critical that these systems and machines be protected from misuse and unauthorized access. This policy applies to all City of Pembroke Pines computer systems and refers to all hardware, data, software, and communications networks associated with these computers. In particular, this policy covers computers ranging from server systems to single user personal computers, whether stand-alone or connected to the network. In addition to this computer policy, users of these computer systems are subject to applicable state and federal laws. Computer abuse will be referred to the Director of Information Technology Services, the City Manager's office and the appropriate Department Head. Computing resources are valuable, and their abuse can have a far reaching negative impact. Computer abuse affects everyone who uses computing facilities. The same morality and ethical behavior that applies in the non-computing environment applies in the computing environment.

II. DEFINITION OF TERMS

A. Computer Systems: Computer systems including any microcomputer (stand-alone or networked), workstation, min-computer, or mainframe computer used by this city or accessible by way of networks, at other locations, computer equipment, computer software, computer accounts, and computer data.

B. The term "computer equipment" will be defined as all electronic and mechanical devices and components connected to the City of Pembroke Pines computer network or connected to City-owned microcomputers.

C. The term "computer software" will be defined as all computer software, City-owned or otherwise.

D. The term "computer data" will be defined as all data residing on City-owned computer equipment.

E. The term "computer account" will be defined as user-IDs, passwords, and other related security information used to authorize access to the computer system.

F. Computer Networks: Computer networks include any local or wide area communications systems connecting computer systems as defined above.

G. Local Area Networking Media: Local area networking media may consist of copper wire, fiber optic cable, thin or thick cable which is used to connect one terminal, microcomputer, workstation, etc. to another or to network interface equipment.

H. Internet: A vast international computer network of many component networks. It contains the ability for electronic mail (e-mail), network news, file and image transfer and information browsing.

I. World Wide Web- (WWW): The more graphical based component of the internet that encompasses many thousands of text, graphic, audio and video files interlinked throughout the world.

III. COMMON FORMS OF COMPUTER ABUSE

Misuse or abuse of computers, computer systems, computer networks, programs and data are prohibited. The following topics are considered areas of abuse:

A. PRIVACY: Violations include, but are not limited to:

(1) Attempting to access another user's computer files without permission;

(2) Supplying or attempting to supply false or misleading information or identification in order to access another user's account;

(3) Deliberate unauthorized attempts to access or use City of Pembroke Pines computers, computer facilities, network systems, programs, or data;

(4) The unauthorized capturing of computer network data directly from network backbone or local area networking media;

(5) Knowingly or carelessly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes programs known as computer viruses and worms.

(6) Attempting to circumvent data protection schemes or uncover security loopholes and/or decrypt intentionally secure data.

B. HARASSMENT: Harassment of other users may be sending of unwanted messages or files. Violations include, but are not limited to:

(1) Interfering with the legitimate work of another user;

(2) The sending of abusive or obscene messages via computers;

(3) Displaying sexually explicit, graphically disturbing, or sexually harassing images or text in a public computer facility, or location that can potentially be in view of other individuals.

C. THEFT: Theft includes the stealing of any property of the City of Pembroke Pines. Violations include, but are not limited to:

(1) Abusing specific computer resources, such the INTERNET or the World Wide Web (as described in other publications);

(2) Attempting unauthorized access to computers outside the City of Pembroke Pines using the City of Pembroke Pines computers or communications facilities;

(3) Removing any computer equipment (hardware, software, data, etc.) without written authorization;
(4) Copying, or attempting to copy, data or software without proper authorization;
(5) Violating terms of applicable software licensing agreements or copyright laws.

D. VANDALISM: Any user's account, as well as the operating system itself, is a possible target for vandalism. Attempted or detected alteration of user system software, data or other files, as well as equipment or resources disruption or destruction, is considered vandalism. Violations include, but are not limited to:

(1) Sending either mail or a program which will replicate itself or do damage to another user's account;
(2) Tampering with or obstructing the operation of the City of Pembroke Pines computer systems (for example, attempting to "crash" the system);
(3) Inspecting, modifying, or distributing data or software without proper authorization or attempting to do so;
(4) Attempting to interfere with the performance of the system;
(5) Damaging computer hardware or software;
(6) Deliberately wasting/overloading computing resources. This includes, but is not limited to, printing multiple copies of a document or printing out large documents that may be available on-line, or that might impact significantly on other users printing resources.
(7) Storing large files on the system which could compromise system integrity or preclude other user's right of access to disk storage. The IT staff may remove or compress disk files that are consuming large amounts of disk space, with or without prior notification.

E. UNAUTHORIZED BUSINESS USAGE: Unauthorized Business Usage includes any use of City of Pembroke Pines resources for promoting or conducting business for personal use. Violations include, but are not limited to:

(1) Sending mass mailings
(2) Using computer accounts for work not authorized for that account
(3) Using your account for any activity that is commercial in nature. Commercial activities include, but are not limited to, consulting, typing services, and developing software for sale.

F. COPYRIGHT ISSUES: The City of Pembroke Pines owns licenses to a number of proprietary programs. Users who redistribute software from the computing break agreements with its software suppliers, as well as applicable federal copyright, patent and trade secret laws. Therefore, the redistribution of any software from computing systems is strictly prohibited except in the case of software, which is clearly marked as being in the public domain. Violations include, but are not limited to copying, transmitting, or disclosing data, software or documentation without proper authorization.

G. MISCELLANEOUS: Other users commonly considered unethical, such as:

(1) Unauthorized and time consuming recreational game playing;
(2) Using computer accounts for work not authorized for that account;
(3) Sending chain letters or unauthorized mass mailings;
(4) Using the computer for any illegal purposes.

IV. PROHIBITIONS

City of Pembroke Pines employees are prohibited from participation either directly or indirectly in the following activities:

A. Use of any computer equipment, computer software, computer data, or computer accounts for unauthorized, illegal, or personal purposes.
B. Unauthorized possession, duplication, distribution, or installation of computer equipment, computer software, computer data, or computer account information.
C. Knowingly gaining access, attempting to gain access or circumvent security, or allowing unauthorized access to computer equipment, computer software, computer data, or computer accounts.
D. Unauthorized addition, deletion, or alteration of computer software, or computer accounts.
E. Knowingly introducing a set of instructions, programmatic or otherwise into computer equipment so as to cause damage to computer equipment, computer software, or computer data.
F. Unauthorized connecting, disconnecting, tampering, or making changes to physical components of computer equipment.
G. Unauthorized changes to computer equipment operating system settings.
H. Failure to respect all copyrights, proprietary rights, or software licensing agreements of computer software or computer data.
I. Using computer equipment or computer software for the purposes of eavesdropping.
J. Sending electronic mail in such a way that it appears to be sent by another person.
K. Anonymous use or use of pseudonyms on a computer system to escape responsibility for their actions or to escape from prosecution of laws and regulations.
L. Sending obscene, harassing, threatening, or defamatory email.
M. Failure to protect the confidentiality and privacy of computer data.
N. Failure to retain computer data in accordance with Florida Public Records Law and State retention scheduled for public records.
O. Failure to notify Data Processing if an employee suspects someone of violating this policy.

V. COMPUTER USAGE GUIDELINES

A. Users are to have valid, authorized accounts and may only use those computer resources which are specifically authorized. Users may only use their account in accordance with its authorized purpose. Users are responsible for safeguarding their own computer account. Users should not let another person use their account unless authorized by the system administrator for a specific purpose. Passwords should be changed often to ensure that private and secure files are kept secure.

B. Users may not change, copy, delete, read, or otherwise access files or software without permission of the custodian of the files or system administrator. Users may not bypass accounting or security mechanisms to circumvent data protection schemes. Users may not attempt to modify software except when intended to be user customized.

C. Users may neither prevent others from accessing the system nor unreasonably slow down the system by deliberately running wasteful jobs, playing games, engaging in non-productive or idle chatting, or sending mass mailings or chain letters.

D. Users shall assume that all software is copyrighted. They may neither distribute copyrighted material without the written consent of the copyright holder not violate copyright or patent laws concerning computer software, documentation or other tangible assets.

E. Users must not use the computer systems to violate any regulations of the City of Pembroke Pines or any state or federal laws.

F. A user shall disclose to the appropriate authorities misuses of computing resources of potential loopholes in computer systems security and cooperate with the City of Pembroke Pines in the investigation of abuse. **In connection with inquiries into possible abuses, the City of Pembroke Pines reserves the right to examine files, programs, passwords, accounting information, printouts or other computing material without notice.**

VI. PENALTIES

Abuse or misuses of computing services may not only violate this policy, but it may also violate the criminal statutes. Therefore, the City of Pembroke Pines will take appropriate action on response to user abuse or misuse of computing services. Action may include, but not necessarily be limited to:

(1) Disciplinary action of the offending computer user by the City of Pembroke Pines;
(2) Reimbursement to the City of Pembroke Pines for resources consumed;
(3) Other legal action including action to recover damages;
(4) Referral to law enforcement authorities.

VII. DISTRIBUTION OF THIS POLICY

The City of Pembroke Pines will insure that all users are aware of the policy by publishing it in appropriate media designed to reach all employees of the City.

H:\760185.PP\MISC\Policy on Use of Computers and Data Communications.doc

INTERNET POLICIES AND GUIDELINES

POLICIES AND GUIDELINES ON THE USE OF CITY INFORMATION SYSTEMS

I. Purpose/Scope

The City of Pembroke Pines ("City") is making every effort to provide its employees with the best technology available to conduct the City's official business. In this regard, the City has installed, at substantial expense, equipment such as computers and advanced technological systems such as electronic mail (e-mail) for use to conduct its official business. This document was created to advise all users regarding the access to and the disclosure of information created, transmitted, received and stored via the use of the Internet, City e-mail, and other Computer systems (collectively referred to as the "City's information systems"). For the purposes of these policies and guidelines, the City's information systems do not include those computer systems designed to be confidential, so long as they are not put on the Internet or Web.

The City's policy regarding the use of the Internet and e-mail, is amount other things, intended to guide you in the performance of your duties as a City employee. It is also intended to place you on notice that you should not expect the Internet or e-mail in your possession or those that you use from time to time, and their contents, to be confidential or private. All data, including any that is stored or data printed as a document is subject to audit and review. ~~**THERE IS NO EXPECTATION OF PERSONAL PRIVACY IN THE USE OF THE INTERNET AND E-MAIL.**~~ **No expectation of privacy- All computers and related equipment are property of the City. The City provides computers and related equipment to employees for use and performing their job functions and for business purposes. As such, employees shall have no expectation of privacy when using City computers and/or related equipment for any purpose. Employees shall not have any expectation that any material or data contained in any portion of the computer or related equipment, which includes email messages and history of Internet use, will be either private or confidential, and as a condition of employment, to the City's interception of all such material, data, and communications.**

Accordingly, the City reserves the right to monitor Internet use, all e-mail, and other computer transmissions, as well as any stored information, created or received by City employees with the City's information systems. The reservation of this right is to ensure that public resources are not being wasted and to ensure that public resources are not being wasted and to ensure that the City's information systems are operating as efficiently as possible in order to protect the public interest. All computer applications, programs, work-related information created or stored by employees on the City's information systems, are City property.

The use of public resources for personal gain and/or private use, such as but not limited to, outside employment, or for political campaign purposes by City employees is prohibited and punishable by disciplinary action. Such disciplinary action may include termination and/or criminal prosecution depending on the nature and severity of the transgression. The term public resource as used in this policy includes not only the unauthorized use of equipment, hardware, software or other tangible articles, but also the employee time spent engaging in the unauthorized use while on duty.

The Florida Public Records Act (FPRA) requires the City to make all public records available for inspection and to provide copies upon request. A public record is any writing (which includes electronic documents) relating to the conduct of the public's business prepared, owned, used, or retained by the City. The FPRA includes a number of exceptions from the disclosure requirement. Any information on the City's information system may be subject to disclosure under FPRA. If there is some doubt, the employee should contact his or her department management, or through proper channels, the City Attorney for advise as to whether the information is a public record.

This document addresses general Citywide Internet policies, specific issues related to appropriate content and use of departmental pages, and employee use of the Internet and e-mail. All departments and employees are required to follow these general policies and guidelines. Specific departments may have unique requirements and are encouraged to develop policies to cover those issues. The law and associated policy regarding the use of Internet, e-mail, and voice mail are continually evolving. Accordingly, review of the policies and guidelines will occur with regularity, and changes shall be made as required.

All Department Heads and Division Directors are responsible for their respective employees' use of the Internet and for contents if their department's information presented using these media. Department and Divisions are encouraged to actively pursue electronic means of presenting information and services to the public.

ALL CITY EMPLOYEES WITH ACCESS TO EMAIL AND/OR THE INTERNET ARE REQUIRED TO READ, UNDERSTAND AND ABIDE BY THE CITY'S POLICIES.

II. City-Wide Internet Policy

The City of Pembroke Pines (City) encourages its departments to use the Internet to disseminate information to the public and its employees (collectively called "users") to improve communications with the public, and to carry out official business when such business can be accomplished consistent with the following Internet policies and guidelines:

- ***Official City Business***- Use the Internet to accomplish official City business consistent with the City's mission. Official City business conducted via the Internet shall comply with all statutory requirements as well as standards for integrity, accountability, and legal sufficiency. Thus, official City business conducted via the Internet should meet or exceed standards of performance for traditional methods (such as meetings, use of telephone, etc.). Internet access for all employees must be authorized through the City Manager's Office.
- ***Reasons to use the Internet***- Departments should base decisions to use the Internet on sound business practices. The conduct of business via the Internet is particularly compelling where costs are reduced and/or the services provided to the City's constituents are improved in measurable ways.
- ***Ease of Use***- Information and services presented via the Internet should emphasize ease of use to reach the broadest audience and impart a friendly manner which would include clear choices, easy navigation, on-screen instruction, etc.

- ***Information Management-*** Disseminate information that is current, accurate, complete, and consistent with City policy. Information released via the Internet is subject to the same official City policies for the release of information via other media (such as printed documents), so that the information disclosed avoids potential problems with copyrights, trademarks, and trade secrets. Information accuracy is particularly important on the Internet. Whether paper-based information is often not current, information presented electronically is much easier to keep current. Constituents expect this information to be not only current but often to be the first available.
- ***Privacy and Security-*** Protect confidential and proprietary information entrusted to the City. Questions regarding confidential and proprietary information should be directed to the department head or his/her designee. City Management has the right to monitor and log all transactions in or out of the system.
- ***Professional Image-*** Use the Internet to promote a professional image for the City.
- ***Official Use-*** Internet resources are made available to City employees to support and promote official City business. It is inappropriate for employees to use these resources for personal use, private gain, to state as "city positions" those which are not officially endorsed by the City, illegal purposes or for inappropriate use as defined in these policies and guidelines. The department heads will be held responsible for the content of their Departments' websites, for ensuring that the information provided relates to their Department's official duties and responsibilities, and that its use is for official and not for personal purposes.

Accordingly, all City Departments should conduct all existing City business using the above policies.

III. City-wide Web Site Policies

A. Purpose

The external (or public) City of Pembroke Pines World Wide Web site is a fundamental communication tool for providing critical City information to residents and the world. The goal of the City of Pembroke Pines Web site is to encourage increased "user" participation in City government and to help create a more vibrant community for residents and visitors alike. The internal (Intranet) web sites provide fundamental and critical information to all employees to assist in accomplishing the City's mission.

Toward that end, the development and use of the City's sites are guided by the Web Site Policy.

B. Policies

(1) The City's Information Technology Division (IT) is responsible for advising City departments regarding the creation and implementation of heir respective Web sites, helping City departments to comply with the City's Web policies, and maintaining and securing the City's Web servers and Web site. It is the responsibility of department heads to ensure that departmental staffs adhere to the Web Site Policies.

(2) To preserve the public nature of the City's Web site and to avoid any perception that the City endorses or provides favorable treatment to any private person or business enterprise (hereinafter collectively referred to as "vendor"), no corporate or commercial logos or links to vendor sites will be allowed on the City's external Web site. When a service has been donated by a vendor that enables the development or maintenance of a City department's initial page (subject to approval from the City Manager's Office) and must include the following statement: "Acknowledgement of (xxxxx) on this page does not constitute the City's support or endorsement of is products or services."

This requirement does not supersede any other policies or regulations regarding donations. Department heads will be responsible for complying with those policies and regulations and seek any required approval for accepting such donations.

(3) Vendors that create or maintain a home page for any City department must follow all policies established for the City's web site.

(4) It is the City's intent to provide electronic access to its information through a logical single point of entry. For the Internet, this logical point of entry is the City's officially registered domain name and each City department or City organization is defined as a sub-area within the official domain. The registration of an individual domain name for a City department or a City-related organization is discouraged because each separate domain name fragments the single logical point of entry, would lead to public confusion, and would contribute to administrative, maintenance, and mail delivery problems. In addition, statistics would be more difficult to compile.

If a specific domain name is required for a City department, a request should be submitted to the Information Technology Steering Committee for review and recommendation to the City Manager. Upon approval by the City Manager, IT will process the registration request.

(5) The City's Web site is for "official use" only. All information disseminated through the City's Web site must be related to the official duties and responsibilities of employees and City departments.

(6) The Florida Public Records Act applies to information processed, sent and stored on the Internet. Confidential information should not be posted on the City's external Website. Each department head must approve all posted information. Questions regarding the Florida Public Records Act shall be routed through appropriate channels to the City Attorney.

(7) In addition to the requirements of policy six (6) above, each department head is responsible for the acceptability of the content contained in their respective Web sites.

(8) No City official's web site may be used for campaign-related purposes. No City employee or official may use any other City departmental Web site for campaign-related purposes. Such campaign-related purposes include, but are not limited to, the following: statements in support or opposition to any candidate or ballot measure; requests fir campaign

funds or references to any solicitations of campaign funds; and references to the campaign schedule or activities of any candidate. The City Attorney is available to provide guidance and assistance to elected officials and their staffs in complying with this guideline. No City official's web site may link directly to the home page of the Office of the City Clerk's election-related pages. Further, the City Attorney is available to provide similar guidance and assistance to the City's department heads.

(9) To encourage participation in and heighten voter interest regarding City elections, the Office of the City Clerk will be responsible for providing candidate, ballot and voter information on its web site and will seek ways to provide similar election-related information via that site.

III. Employee's Internet Usage Policy

The following rules require strict adherence. Any infraction thereof could result in disciplinary action. Disciplinary actions range from verbal warnings to termination, the severity of the disciplinary action will be governed by the nature of the offense, prior disciplinary action and any legitimate mitigating circumstances that may exist.

(1) The use of Internet is restricted to "official City business". ~~Personal use and/or time spent for personal gain is strictly prohibited.~~ Authorization for Internet access must be obtained through the City Manager's Office. Once authorization is approved you are responsible for the security of your account password and you will be held responsible for all use or misuse of your account. You must maintain secure passwords and never use an account assigned to another user.

(2) Personal Use of Computers and Related Equipment- Use of City computers and related equipment is limited to performing job functions and for business purposes. Subject to the requirements of this policy, incidental and occasional personal use of the City computers and related equipment is permitted. However, any use of City computers and related equipment that interferes with or causes a delay in the performance of the employee's responsibilities or work shall be a violation of this policy. Moreover, such personal use shall conform with the City's standards of conduct for City employees, not violate any other City policies, or cause added expense to the City.

(3) Hacking is the unauthorized attempt or entry into any computer. Never make an unauthorized attempt to enter any computer. Such an action is a violations of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.

(4) Sending threatening, slanderous, racially and/or sexually harassing messages is strictly prohibited.

(5) The representation of you as someone else, real or fictional or a message sent anonymously is prohibited.

(6) Never copy or transfer electronic files without permission.

(7) Never send, post, or provide access to any confidential City materials or information.

(8) Almost all data and software is subject to the Federal copyright laws. Care should be exercised whenever accessing or copying any information that does not belong to you. Software that requires purchase or reimbursement for its use, such as shareware, requires

strict adherence to the terms and conditions specified by the owner unless written permission for unrestricted use was obtained. When in doubt consult your department head or designee.
(9) You are obliged to cooperate with any investigation regarding the use of your computer equipment.
(10) Chain letters are illegal and may not be transmitted through e-mail.
(11) E-mail requires extensive network capacity. Sending unnecessary e-mail, or not exercising constraint when sending very large files, or sending to a large number of recipients consumes network resources that are needed for critical City business. When the City grants an individual employee access to the network, it is the responsibility of the employee to be cognizant and respectful of network resources.

V. Employee's Internet Usage Guidelines

A. Internet Sites

(1) If you are using information from an Internet site for strategic City business decisions, you should verify the integrity of that information. You should verify whether the site is updated on a regular basis (the lack of revision date might indicate out-of-date information) and that is a valid provider of the information you are seeking. Just because it is there does not mean that it is accurate or valid.
(2) IT has not control or responsibility for content on an external server not under the control of the City of Pembroke Pines. Information may be offensive and/or unsuitable for dissemination.

B. Electronic Mail (E-mail)

The following guidelines apply to the use of e-mail:

(1) ***MAIL ON THE INTERNET IS NOT SECURE***- Never include anything in an e-mail message that you want to keep private and confidential. E-mail is sent unencrypted and is easily read.
(2) Management has the right to access all e-mail files created, received or stored on City-funded systems and such files can be accessed without prior notification.
(3) Be careful if you send anything but plain ASCII text as e-mail. Recipients may not have the ability to translate other documents, for example Word or Word Perfect documents, or encoding in UUENNCODE or MIME
(4) Be careful when sending replies- make sure you are sending to a group when you want to send to a group and to an individual when you want to send to an individual. It is best to address directly to a sender(s). Check carefully the "To" and "From" before sending mail. It can prevent unintentional errors.
(5) Include a signature (an identifier that automatically appends to your email message) that contains the method(s) by which others can contact you (usually your e-mail address, phone number, fax number, etc.).
(6) For important items, let senders know you have received their e-mail, even if you cannot respond in depth immediately. They need to know their e-mail is not lost.

(7) Watch punctuation and spelling. It can reflect on your professionalism. Use automatic checking programs if available.

C. Internet Mailing Lists and Usenet News Groups

The e-mail guidelines apply here as well:

(1) Actively disclaim speaking for the City of Pembroke Pines unless you have authority to do so. Note that if you use a City of Pembroke Pines system to post an article, the City's name is carried along with what you post in (at least) the headers. The "standard" disclaimers attached to many articles are meaningless if the reader finds the article offensive.
(2) Be sure to change your mailing address if you account changes. Do not simply forward your e-mail from your old account to your new one. This creates a burden on the City's information systems. Be careful when using auto-reply features in e-mail when you belong to mailing lists. Auto-reply replies are often sent to the entire list indiscriminately and your reply may not be important to all on the list; e.g. most do not care that you are on vacation, and worse, your message may have been intended for only one recipient.
(3) As a new member of a *news group*, monitor the messages for a while to understand the history and personality of the group. Jumping right into the discussion may make you look foolish if you lack background information.
(4) Do not re-post any messages without permission. Even messages may have copyright protection.
(5) Do not post personal messages to a mailing list or news group.
(6) If you survey the group, as a courtesy, post a summary of the results.
(7) Be sure to properly acknowledge with quotations any material borrowed from others. Be careful of plagiarism.
(8) Do not post any messages anonymously. The professional community views this practice as bad form. As a matter of policy the USENET community and systems managers are asked to track down offenders.
(9) Be careful when you re-post and requests. Some requests are fraudulent.
(10) State the subject of your message clearly in the subject line.
(11) Before joining mailing lists and news groups give thought to how much time these activities require.
(12) Be sure to read the Frequently Asked Questions (FAQs) for your group(s).
(13) Never send angry messages (flames). If you receive a "flame", do not overreact. Remember that not everyone is as polite as you are.

D. FTP (File Transfer Protocol)

These guidelines cover use of FTP (or download) sites):
(1) Do not FTP to any system on which you do not have an account, or which does not advertise anonymous FTP services.
(2) Observe working hours or posted hours for FTP sites. Most sites request that you not FTP between their local hours of 8am-5pm.
(3) Do not FTP during your site's prime hours due to network impact on other users. (IT is exempt)

(4) Observe any posted restrictions on the FTP server.

E. TELNET

These guidelines cover the use of TELNET:

(1) Do not TELNET to machines on which you have no account, or where there is no guest account. Do not attempt to TELNET deliberately into anonymous FTP servers.
(2) When you TELNET observe any posted restrictions.
(3) Do not attempt to TELNET into ports without authorization.

F. Netiquette

These are Netiquette (see Glossary) guidelines:

(1) Be cognizant of system etiquette. The computer you may use may have limits regarding disk space usage. E-mail takes up space; therefore, you should regularly delete and/or archive any messages you wish to save.
(2) Remember that the recipient is a person with feelings. Since they cannot see you, they may not know when you are joking. Be sure to include visual or verbal clues. Convention indicates the use of the smiley face. :) (Look sideways).
(3) DO NOT SEND MESSAGES ALL IN CAPITALS. It looks as if you are shouting. Use initial capitals or some symbol for emphasis. For example: That IS what I meant. That "is" what I meant.
(4) Remember that some people have to pay for each byte of data they receive. Please keep messages to the point without appearing terse or rude.

VI. GLOSSARY

Domain Name:
A domain name is the way to identify and locate an address on the Internet. The domain name, also called the fully-qualified domain name or FQDN, is a computer's name in text form, for example: ppines.com. The domain name is used to send e-mail, make FTP requests, etc. Before any message is sent on the Internet, the domain name is converted internally to a numerical address, an Internet protocol address, which is what computers on the Internet deal with directly.

Electronic Mail:
Electronic mail (e-mail) may include non-interactive communication of text, data, images, or voice messages between a sender and designated recipient(s) by systems utilizing telecommunications links. It may also include correspondence transmitted and stored electronically using software facilities called "e-mail", "facsimile", or "messaging" system; or voice messages transmitted and stored for later retrieval from a computer system.

FTP:
File transfer protocol; a program that allows you to transfer data between different computers on a network.

Guidelines:
Recommendations derived from experience and which should be used.

Hacking:
Attempting to break into system on which you have no account or authorization.

Internet:
A worldwide network or networks, connecting informational networks communicating through a common communications language or "protocol".

Mailing list:
A service that sends e-mail to everyone on a list whenever e-mail is sent to the service, permitting a group of users to exchange e-mail on a particular topic.

MIME:
A protocol which lets Internet users attach non-text files to e-mail messages. Stands for Multipurpose Internet Mail Extension, lets users send mail in any format including graphic images, formatted documents, and audio, video and compressed data files.

Netiquette:
A combination of "network" and "etiquette". It is the practice of good manners in a networked environment.

News groups:
Discussion groups with common themes on USENET.

Policy:
Primary objectives of the City of Pembroke Pines as contained in this document.

Standards:
Departmental directions or instructions describing how to achieve policy. A mandatory statement of direction.

TELNET:
A program that allows remote login to another computer.

TCP/IP:
Transmission Control Protocol/Internet Protocol; the communication protocol used by computers connected to the Internet.

USENET:
A collection of computer discussion (news) groups.
Users:
The public and City employees.

UUENCODE:
A utility that converts binary files on PC into ASCII files. Stands for Unix-to-Unix Encode and was first developed for use with UNIX computers.

Vendors:
Any private person or business enterprise.