



CITY COUNCIL
Administrative Oversight
& Land Use Committee

Monday, May 3, 2010
5:00 pm
City Council Office

COMMITTEE OF THE WHOLE

5:00 pm

- I. Review Draft Response Letter re Bernhart's Park Remediation Plan**
- II. Business License Revocation Ord. Tabled at 4-26 Reg. Mtg.**

I. Interviews

6:00 pm

- 6:00 - **Becky Acosta** - appointment - Reading Housing Authority
- 6:15 - **Thomas Anewalt** - appointment - Legislative Aide Committee
- 6:30 - **Lisa Blount** - reappointment - Human Relations Commission
- 6:45 - **Twila Ramirez** - appointment - Legislative Aide Committee
- 7:00 - **Lynn Smith** - appointment - Animal Control Board alternate
- 7:15 - **Russell Manbeck** - reappointment - Disruptive Conduct Review Board

II. Appointment Recommendations

III. Review Pending Applications Memo/BAC Openings

IV. Computer Policy re E Mail Review and Audit

- V. Bill No. 22-2010** – authorizing the City to enter into an Intergovernmental Agreement for the purpose of providing mutual aid among the County of Berks, the

Friendship Hook and Ladder Company No. 1 of Boyertown, PA, the City of Reading and the Township of Spring to assist first responders in the mitigation of emergencies related to trench and structural collapse **(Law) Introduced at the April 12 regular meeting – Tabled at 4-26 Reg. Mtg. – re ability of individual parties to withdraw from mutual aid agreement**

Upcoming Topics

Zoning Ordinance Amendment - *underway*

SALDO - *underway*

Review of enabling legislation for 2 Boards, Authorities & Commissions per year

City of Reading Computer and Network Use Policy

Updated and Revised February 2004

Acquisition of Software

All software acquired by the City of Reading (“The City”) must be purchased through the Information Technology Division (“IT”), or its designee, and the Purchasing Division. Software may not be purchased through any other means. Software acquisition is restricted to ensure that the City has a record of all software that has been purchased for City computers and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

Registration of Software

When the City receives the software, IT, or its designee, must receive the software first to complete registration and inventory requirements before installation. Software must be registered in the name of ITD, City of Reading. IT maintains a database of all software and the quantity owned.

Installation of Software

All software will be installed by IT, or its designee. Once installed, the original media will be kept in an area determined by IT. User manuals will either reside with the pc/server or reside within IT.

Home Computers and Software

Users are not permitted to bring software from home and load it onto City equipment. City owned software cannot be taken home and loaded on a user's home computer without prior written permission from IT. If a user needs to use software at home, they should consult with the Information Technology manager, through their supervisor, to determine if the software licenses permit home use and the use is warranted.

Non-City Owned Equipment

Users are not permitted to bring computer equipment or equipment capable of interfacing to computer equipment and/or systems (Laptops, PC's, etc.) from home or any other location for use on City property or for City business without prior departmental approval and written notification to IT by the applicable department of the purpose of the equipment, location of its intended use and name(s) of the individual(s) using said equipment. Any equipment found on City property, without the appropriate approval, may be confiscated and delivered to the appropriate department director.

Shareware/Freeware

Acquisition and registration of shareware/freeware products will be handled the same way as for all other software acquisition.

Audits

IT conducts random, unannounced audits of City equipment and systems to ensure that the City is in compliance with all software licenses and policies. Any such audits would be performed on City property. The City of Reading reserves the right to inspect any City system and/or device for any reason.

Viruses

IT will search for computer viruses using various methods and eliminate any that are found. Users are not to modify, adjust or tamper with any virus software that resides on any City computer system. The introduction of viruses, or malicious tampering with any computer system, is expressly prohibited. Files that are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to detect for a virus and, if necessary, to prevent its spread. Any “infected” file found in any server will be automatically purged from the system without warning.

Software

All users will use all software in accordance with its license agreements. All users acknowledge that they do not own this software or its related documentation, and unless expressly authorized by IT, may not make additional copies.

No user will give software, folders, files or fonts to anyone outside the City including but not limited to clients, customers, and others. Under no circumstances will software be used within the City that has been brought in from any unauthorized location under the City policy, including, but not limited to, the Internet, the home, friends and colleagues.

Any user who determines that there may be a misuse of software within the City will notify IT in writing

E-mail

Messages that are created, sent, or received using the City’s e-mail system are the property of the City of Reading.

The City reserves the right to access and disclose the contents of all messages created, sent, or received using the e-mail system.

The E- mail system is strictly for official City messaging. Personal broadcast messages are in violation of the official policy of The City of Reading.

Email Attachments that are not work related, i.e. any executables, movies or visual basic scripts are prohibited and will be purged from the system.

Monitoring and/or Recording of Electronic Communication

All electronic communications throughout the City Network(s) is/are monitored, recorded and subject to review by IT. These would include but are not limited to Email, Internet, Instant messaging, Chat and any systems and/or capabilities that are added in the future.

All users should have no expectation of privacy while using any system or sub-system of the City of Reading network.

Internet

It is the policy of the City to limit Internet access to official business. Employees are authorized to access the Internet, for personal business, after- hours, in strict compliance with the other terms of this policy. The access to any pornographic material, web sites, etc is strictly prohibited. Internet usage is monitored by the IT Division.

Employees using City accounts are acting as representatives of The City of Reading. As such, employees should act accordingly so as not to damage the reputation of the organization.

Employees shall not place company material (copyrighted software, internal correspondence, etc.) on any publicly accessible Internet computer without prior permission.

Alternate Internet Service Provider (ISP) connections to the city network are not permitted unless expressly authorized by IT and properly protected by a firewall or other appropriate security device(s).

Sensitive material will not be transferred over the internet without prior departmental approval.

Employees are prohibited from downloading software and/or modifying any such files without permission from IT.

Security

Unauthorized attempts to gain privileged access or access to any account, system, file or folder not belonging to the user is prohibited. Any user found in violation will have the system account disabled without notification.

Users are not to give out or share account usernames and/or passwords to/with anyone.

Any violations will result in the account being disabled.

All users will be held accountable for any activity attempted or completed with their username.

Modem Access

Dialing in or out of the City network via modem, or any other means, is prohibited without the prior approval of IT.

Equipment Liability/Abuse

Individual users will be required to sign the Equipment Liability Form for any equipment issued or loaned to them, regardless of the purchasing entity. The user is responsible for all damage and/or loss of any equipment issued or loaned.

Any equipment that is issued to a department for the use of multiple users will be the responsibility of the department using the equipment.

This section does not apply to normal “wear and tear” of equipment or defective equipment.

Penalties

According to the US Copyright Act, illegal reproduction of software is subject to civil damages of as much as \$150,000 per title infringed, and criminal penalties, including fines of as much as \$250,000 per title infringed and imprisonment of up to five years.

A City user, who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate. Such discipline may include termination of employment. Any unauthorized activity by an employee may be the responsibility of the organization.

Therefore, the City may choose to hold the employee(s) liable for their actions.

The City of Reading Computer and Network Use Policy supercedes any and all departmental policies and is subject to modification. If any modifications are made all individuals who signed prior revisions will be notified by email and/or memorandum of any changes and what the changes are. Any questions regarding this policy should be directed to the Information Technology manager.

By signing below, I indicate that I have read, fully understand and agree to abide by The City of Reading Computer and Network Use Policy.

First Name Middle Initial Last Name

Department Signature

Date

Definitions

- 1. City Equipment: Any piece of equipment or software purchased by the City of Reading through any means, i.e.: general funds, capital funds, grant purchases, donated equipment, etc.
- 2. Defective Equipment: IT staff shall define if an equipment failure is a manufacturing defect or abuse.

Computer and Internet Use

Internet access to global electronic information resources on the World Wide Web is provided by City of Sunbury to assist employees in obtaining work-related data and technology. The following guidelines have been established to help ensure responsible and productive Internet usage. While Internet usage is intended for job-related activities, incidental and occasional brief personal use is permitted within reasonable limits.

All Internet data that is composed, transmitted or received via our computer communications systems is considered to be part of the official records of City of Sunbury and, as such, is subject to disclosure to law enforcement or other third parties. Consequently, employees should always ensure that the business information contained in Internet e-mail messages and other transmissions is accurate, appropriate, ethical and lawful.

The equipment, services and technology provided to access the Internet remain at all times the property of City of Sunbury. As such, City of Sunbury reserves the right to monitor Internet traffic and retrieve and read any data composed, sent or received through our on-line connections and stored in our computer systems.

Data that is composed, transmitted, accessed or received via the Internet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation or any other characteristic protected by the law.

The unauthorized use, installation, copying or distribution of copyrighted, trademarked or patented material on the Internet is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it, or has not gotten authorization for its use, it should not be put on the Internet. Employees are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights.

Internet users should take the necessary anti-virus precautions before downloading or copying any file from the Internet. All downloaded files are to be checked for viruses; all compressed files are to be checked before and after decompression.

Abuse of the Internet access provided by City of Sunbury in violation of law or City policies will result in disciplinary action, up to and including termination of employment. Employees may also be held personally liable for any violations of this policy. The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

1. Sending or posting discriminatory, harassing, or threatening messages or images
2. Using the organization's time and resources for personal gain
3. Stealing, using, or disclosing someone else's code or password without authorization
4. Copying, pirating, or downloading software and electronic files without permission
5. Sending or posting confidential material, trade secrets, or proprietary information outside of the organization
6. Violating copyright law
7. Failing to observe licensing agreements
8. Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions
9. Sending or posting messages or material that could damage the organization's image or reputation
10. Participating in the viewing or exchange of pornography or obscene materials

11. Sending or posting messages that defame or slander other individuals
12. Attempting to break into the computer system of another organization or person
13. Refusing to cooperate with a security investigation
14. Sending or posting chain letters, solicitations, or advertisements not related to City purposes or activities
15. Using the Internet for political causes or activities, religious activities, or any sort of gambling
16. Jeopardizing the security of the organization's electronic communications systems
17. Sending or posting messages that disparage another organization's products or services
18. Passing off personal views as representing those of the organization
19. Sending anonymous e-mail messages
20. Engaging in any other illegal activities

E-mail Contents

The Electronic Mail ("E-mail") system provided by the City is the property of the City and is provided for the purpose of conducting City business. You should not assume that Email messages and their attachments are secure or private. E-mail messages may be retrieved by anyone to whom you have given your password, to whom you have given e-mail access rights, or by anyone having access to your computer while you are logged into it. The City reserves the right to read and disclose the contents of E-mail messages for any purpose as a condition of employment or continued employment. Staff waives any right to privacy in E-mail messages and consent to the access and disclosure of E-mail messages by authorized municipal representatives. The City may access and review employee E-mail messages at any time without prior notice.

It is the policy of the City that any communication by E-mail should be drafted with the same care as a formal memorandum and should not contain informal remarks that might potentially be embarrassing to the sender, the receiver, the staff, or the City. The contents of E-mail should not include anything which the sender would not want publicly disclosed.

- E-mail should not be used for personal communications.
- E-mail should not be used to discuss confidential or sensitive information relating to employees or residents.
- E-mail should not be used to transmit sensitive or confidential City management, financial, or personnel reports, including medical reports or communications relating to such reports.
- E-mail should never contain offensive or harassing language. This prohibition includes the display or transmission of sexually explicit images, cartoons, jokes, or messages; vulgarities, obscenities, sarcasm or exaggerations. Staff are strictly prohibited from sending E-mail messages of a harassing, intimidating, offensive or discriminatory nature. Such conduct, or any other conduct in violation of this policy, may result in immediate dismissal or other disciplinary measures.
- Email utilizing the computer system of the City is subject to the provisions of the Pennsylvania Open Records Act.

E-Mail Retention

In most cases, e-mail messages should be deleted after they are read. The contents of the In box, Out box, and Trash should be emptied/deleted on a regular basis - at least monthly. Do not use your electronic mail box for permanent message storage.

Under normal circumstances, the City rotates its backup tapes on a regular basis. These backup tapes include copies of the users' E-mail databases. Periodically, all electronic media copies of an e-mail message will be deleted. If the City becomes involved in an investigation, litigation, or any other proceeding which necessitate the review or production of City records, the City may suspend the regular deletion of all or part of e-mail messages for an indefinite period without notice. All employees are required to comply with litigation hold notices.

Ownership of Information Stored on Electronic Media

All information, in any format, stored by any means on the City's electronic facilities (Voicemail, E-mail, computer network drives, hard drives, or individual diskettes) is the property of the City. Do not assume that any electronically stored information is private or inaccessible by others. In addition to periodic, unannounced review of stored material by authorized City employees or contractors, such information might be retrieved by unauthorized persons. When stored information is requested or subpoenaed by persons who do not share ownership of the information, that information should not be provided until thorough consideration has been given to the issues relating to attorney work product and attorney-client privilege theories. In no cases shall it be destroyed without written permission of the City Solicitor.

Use of Phone and Mail Systems

Personal use of the telephone for long-distance and toll calls is not permitted. Employees should practice discretion when making local personal calls and may be required to reimburse City of Sunbury for any charges resulting from their personal use of the telephone.

The mail system is reserved for business purposes only. Employees should refrain from sending or receiving personal mail at the workplace.

To ensure effective telephone communications, employees should always use the approved greeting and speak in a courteous and professional manner. Please confirm information received from the caller, and hang up only after the caller has done so.

Workplace Monitoring

Workplace monitoring may be conducted by City of Sunbury to ensure quality control, employee safety, security, and customer satisfaction.

Computers furnished for employees use are the property of City of Sunbury. As such, computer usage and files may be monitored or accessed.

COMPUTER USE

The City of Meadville recognizes that use of the Internet has many benefits for The City of Meadville and its employees. The Internet and e-mail make communication more efficient and effective. Therefore, employees are encouraged to use the Internet appropriately. Unacceptable usage of the Internet can place The City of Meadville and others at risk. This policy discusses acceptable usage of the Internet.

Guidelines

The following guidelines have been established for using the Internet and e-mail in an appropriate, ethical and professional manner.

1. The City of Meadville Internet and e-mail access may not be used for transmitting, retrieving or storing of any communications of a defamatory, discriminatory or harassing nature or materials that are obscene or X-rated. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. Harassment of any kind is prohibited.
2. Disparaging, abusive, profane, or offensive language; materials that would adversely or negatively reflect upon The City of Meadville or be contrary to The City of Meadville best interests; and any illegal activities -- including piracy, cracking, extortion, blackmail, copyright infringement, and unauthorized access to any computers on the Internet or e-mail -- are forbidden.
3. Copyrighted materials belonging to entities other than those belonging to The City of Meadville may not be transmitted by employees on the City's network. All employees obtaining access to other companies' or individual's materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy to reference only. If you find something on the Internet that may be interesting to others, do not copy it to a network drive. Instead, give the URL (uniform resource locator or "address") to the person who may be interested in the information and have that person look at it on his/her own.
4. Do not use the system in a way that disrupts its use by others. This includes excessive dial-in usage, sending or receiving many large files and "spamming" (sending e-mail messages to thousands of users.)
5. The Internet is full of useful programs that can be downloaded, but some of them may contain computer viruses that can extensively damage our computers. Be sure to virus-check downloaded files immediately. Instructions on how to check for viruses are available through the IT Department. Also, many browser add-on packages (called "plug-ins") are available to download. There is no guarantee that such will be compatible with other programs on the network and such may cause problems; therefore, please refrain from downloading such plug-ins.

6. Each employee is responsible for the content of all text, audio or images that he/she places or sends over the City's Internet and e-mail system. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else. Also, be aware that The City of Meadville's name is attached to all messages so use discretion in formulating messages. Also, be aware that The City of Meadville's name is attached to all messages that are assigned City e-mail accounts, so use discretion in formulating messages.

7. E-mail is not guaranteed to be private or confidential. All electronic communications are The City of Meadville property. Therefore, The City of Meadville reserves the right to examine, monitor and regulate e-mail messages, directories and files, as well as Internet usage. Also, the Internet is not secure so don't assume that others cannot read -- or possibly alter -- your messages.

8. Internal and external e-mail messages are considered business records and may be subject to discovery in the event of litigation. Be aware of this possibility when sending e-mail within and outside the City.

The City of Meadville's right to Monitor and Consequences

All City-supplied technology, including computer systems and City-related work records; belong to The City of Meadville and not the employee. The City of Meadville routinely monitors usage patterns for its e-mail and Internet communications. Although encouraged to explore the vast resources available on the Internet, employees should use discretion in the sites that are accessed.

Since the entire computer systems and software, as well as the e-mail and Internet connection, are owned by the City of Meadville, all City policies are in effect at all times. Any employee who abuses the privilege of the City of Meadville facilitated access to e-mail or the Internet, may be denied access to the Internet and, if appropriate, be subject to disciplinary action up to and including termination.

Town of Bloomsburg Employees And Town Council Members Internet Usage Policy

The Town of Bloomsburg has contracted with an Internet Access Provider to provide access to the Internet on all computers. This Internet access has been obtained and is maintained for Town business purposes. In addition, the Town of Bloomsburg will allow individual employees to use the Town's computers to obtain access to the Internet, during the employee's off-duty hours, under limited circumstances. The following policies apply to all use of the Internet from Town-owned computers or the BAFN's computer system.

1. The BAFN's computer system and access to the Internet is maintained for the purpose of conducting Town business.
2. Employees may be permitted to use the Town of Bloomsburg's computer(s) in order to obtain access to the Internet under the following circumstance.
 - a. The Town of Bloomsburg's computer(s) and Internet access will be provided only during those periods when the computer system is not otherwise needed for Town business.
3. Only Town Council Members and Employees of the Town of Bloomsburg are authorized to use the Town's computer(s) or access the Internet through the BAFN's system, whether for Town business or otherwise. No employee has the authority to authorize or permit others to use the Town's computer(s) for any purpose.
4. The Town employees should use discretion when using e-mail, list-servers, bulletin boards and other such communications other than for Town purposes on the Internet.
5. The use of the Internet to access, download or display pornographic, obscene or otherwise offensive materials is strictly prohibited and will be considered a violation of the Town of Bloomsburg's policy. Before downloading sound bytes, large files and graphics, employees must obtain supervisor authorization.
6. No information or materials related to Town business or operations may be posted on the Internet without prior approval/notification from employees supervisor.
7. The terms of the Agreement between the Town of Bloomsburg and the BAFN apply to all Internet usage by Town Council Members and Town Employees except that the Town makes no assurances of privacy as to any employee's usage of the Town of Bloomsburg's computer(s) or the Internet through the BAFN's computer system. The Town Council

specifically retains the right to review usage of the Town of Bloomsburg's computer(s) and the Internet to assure compliance with this policy.

8. Any employee violating the computer usage policy may be subject to disciplinary action as follows: the first violation is a verbal reprimand, second violation is a written reprimand, third violation is a suspension for three (3) days and the fourth violation of these rules is means for discharge. In addition, the Town Council retains the right to discontinue the policy of permitting access to the Town of Bloomsburg's computer(s) for non-Town business, at any time.

CITY OF LANCASTER
Lancaster, Pennsylvania

SUBJECT: Communications and Use of Communication Systems		
EFFECTIVE DATE: March 1, 2000		
PAGE: 1	Reference: E-Mail & Internet	

PURPOSE: The City of Lancaster is now making available the Internet & E-Mail capabilities to all computers that are connected to the AS400 Network. The accurate and timely exchange of information is vital to any organization. Technology has provided advancements in methods of communication that have dramatically improved the ability to exchange all types of information. Enhanced communication ability offers the potential for any public service agency to greatly improve its efficiency and its accessibility to the public. Communications that are contradictory to the mission of an organization, however, can be internally disruptive, and if made public, can diminish the confidence the public may have in that agency. For that reason, guidelines must be in place that dictate unacceptable communications and unacceptable uses of communication systems.

POLICY: Communications within the City of Lancaster will at all times reflect our mission of maintaining the highest level of professionalism and integrity in providing service to our community. The City will make every effort to take full advantage of communication systems to provide for the most effective and efficient exchange of information and to make the services of the City as accessible to the public as possible.

PROCEDURE: All personnel will observe the following guidelines in complying with this policy:

I. Definitions

- .10 The following terms as used in this policy document and not otherwise defined are defined as:
- A. **Anti-Virus software** is software designed to identify and isolate a computer virus before it can corrupt or otherwise cause damage to computer software or hardware.

- B. **Encryption program** is software designed to or enabled with functionality that prevents persons from accessing data without using a password, code or a decipher program.
- C. **Outside computer** is any computer that has a modem and internet service, such as the Bureau of Streets, Water, Parks, Wastewater Operations, T&D, etc.
- D. **Pirated software** is any copyrighted software that has been illegally copied or duplicated.
- E. **Security feature** is any safeguard, intended to prevent access to a communication system or part thereof, by unauthorized persons and may include, but is not limited to any key, code, password, authorization number, setting, address or telephone number.

II. General Guidelines

- .10 Various communication systems and technologies may be utilized by or provided to City employees.
- .20 Communication systems are provided for the mutual benefit of City employees.
- A. **“Communication systems”** include both contemporaneous and pre-recorded communications.
 - 1. A communication system includes, but is not limited to:
 - i. bulletin boards and other places where documents or messages are posted or stored,
 - ii. telephones,
 - iii. tele-facsimile (fax) devices,
 - iv. voice and video recorders and players,
 - v. cellular telephones,
 - vi. two and three way radio systems,
 - vii. paging systems,
 - viii. electronic mail (e-mail),
 - viii. voice mail,
 - ix. computers and computer systems, and
 - x. Internet

- B. No employee shall access communications unless intended for City business.
- C. No employee will access or alter or attempt to access or alter, any part of a communication system for which they do not have authorization to access or alter, and if done so inadvertently, will immediately notify their supervisor.
- D. All communications will be in English unless the intended recipient does not speak or otherwise understand the English language.
- E. To avoid introduction of a virus, no computer software will be loaded onto or otherwise used on any City computer equipment without approval of the Bureau of MIS.
- F. No **pirated software** will be used at anytime.
- G. No employee will reveal to any unauthorized person, the existence of, functionality of, or means of accessing, defeating, or avoiding any type of **security feature** associated with a communication system.
- H. No classified, confidential, sensitive, proprietary or private information or data shall be disseminated to any unauthorized person, group or organization.
- I. Employees will insure that a current up-to-date anti-virus program, approved by the Bureau of MIS, is running on any **outside computer** the employee is using to transfer information in any manner or form, between computers.

III. Limitation On Use of Electronic Mail (E-Mail)

- .10 Employees should not open e-mail messages unless they are certain of the trustworthiness of the source.
- .20 Suspect messages should be referred to the Bureau of MIS for virus check.
- .30 Employees should not trust e-mail messages to be a secure and confidential means of communications since subsequent directing of the message cannot be controlled.

.40 Employees will not knowingly accept messages with inappropriate content as described in Section VI., and will immediately and completely delete any such message inadvertently received.

IV. **Games** – No games or other programs not used in City business shall be installed by any user on a City computer. Any program installed on a City computer must be checked by MIS before installed.

V. **Limitations on the Use of the Internet**

.10 Access to the Internet is a tool provided to City employees to enhance their ability to perform their jobs, providing almost unlimited research opportunities.

.20 Generally employees will use the Internet for job related research only.

A. Personal use of the Internet will be permitted with permission of a supervisor provided:

1. Such use is infrequent, such as lunch time.

2. Such use is not contrary to any other provision of this policy;

3. Such use does not interfere with an employee's daily business responsibilities.

B. Nothing will be downloaded from the Internet unless the anti-virus program is active and the downloaded is business related.

.30 Employees are reminded that the validity of file information found on the Internet is not generally guaranteed and should be verified before being used.

VI. **Use of Communication Systems Inconsistent with the Mission of the City of Lancaster.**

.10 Communication systems shall never be used in a manner inconsistent with the mission of the City of Lancaster as stated in the Policy statement on page 1.

A. Inconsistent use includes, but is not limited to communications that;

1. threaten or intimidate another person;
 2. images that contain nudity or other images, words, or language that are sexually explicit or of a prurient or sexually suggestive nature unless necessary as part of a criminal investigation approved by the Chief of Police or a Division Captain.
 3. images, words, or language that tends to disparage a person or group because of race, ethnic background, national origin, religion, or for any other reason.
- .20 No City document or written communication, or any document or written communication permitted by City policy, will be marked, marred, defaced or otherwise altered in any fashion.
- .30 No City communication system may be used in anyway to further the private or personal gain of a City employee with the following exception:
- A. Employees may use City tele-facsimile (fax) devices for personal messages only with approval of their Supervisors and provided that:
 1. Such use is infrequent;
 2. Such use is not contrary to any other provision of this policy;
 3. The City is reimbursed for any long distance fees associated with the transmission, and;
 4. Such use does not interfere with or delay the employee's business responsibilities.

VII. No Expectation of Privacy.

- .10 No employee shall have any expectation of privacy when using City authorized or provided communication systems.
- .20 In order to insure compliance with this policy document, the City reserves the right, where not in conflict with any law, to monitor telephone conversations, to read messages, to decipher encrypted text and to remove or inspect software, especially software installed or altered without authorization.
- .30 In order to insure compliance with this policy document, the City reserves the right to access, without notice, data or text caches, pager memories,

e-mail and voice mailboxes and any other City provided electronic system.

- .40 The City does not need to obtain prior judicial approval to monitor or access the communications systems described in this policy document, and an employee's continued employment waives any claims for infringement of privacy.

VIII. Obligation to Report Violations of this Policy

- .10 All employees have an obligation to report to their supervisors, intentional or negligent violations of this policy by another employee.
- .20 Supervisors to whom violations of this policy are reported, will immediately report the violation to their Director, and, Chief of MIS and Bureau of Human Resources.

- IX.** Any violation of these guidelines is cause for disciplinary action up to and including termination.

A definitive policy to cover all eventualities cannot be created. This policy and procedure is meant to serve as a guide to personnel so that they have an understanding of their respective responsibilities and City of Lancaster expectations when using City provided or authorized communication systems and to establish uniform procedures for the use of the systems.

Computer E-mail & Internet Policy

On this date, _____ I have been made aware of and provided a copy of the City of Lancaster Computer Policy.

Signature

*Please return signed document to the HR Office

Any questions regarding this policy should be directed to the HR/MIS Bureaus.

BOROUGH OF WEST CHESTER – Networking Policy

Policies Regarding Ownership of Information Stored On Electronic Media

1. All information, in any format, stored by any means on the Borough's electronic Facilities (voicemail, email, computer network drives, hard disks or individual diskettes) is the property of the Borough and subject to inspection at any time without notice. Do not assume that any electronically stored information is private or inaccessible by authorized Borough personnel. In addition to periodic, unannounced review of stored material by authorized Borough employees, such information might be retrieved by unauthorized persons.

Policies Regarding Computer Software Licenses

1. The Borough of West Chester purchases licenses permitting the use of computer software and shall not knowingly distribute software or make copies of purchased software without the express permission of the vendor.
2. With regard to use of local area network or on multiple machines, the Borough's employees shall use software only in accordance with the license agreement(s).
3. Borough employees learning of any misuse of software or related documentation within the Borough shall notify the Borough Manager or Department Manager.
4. According to U.S. Copyright law, illegal reproduction of software can result in civil damages as much as \$50,000 and criminal penalties including fines and imprisonment. The Borough does not condone the illegal duplication of software.

Policies on Internet Usage

1. The Borough of West Chester has contracted with an Internet Access Provider to provide access to the internet on certain Borough computers. This internet access has been obtained and maintained for Borough business purposes. The following policies apply to all use of the internet from Borough computers or the Borough's Local Area Network.
2. The Borough's computer system and access to the internet is maintained for the purpose of conducting Borough business. Use of Borough computers or the internet during work hours for personal purposes is prohibited.
3. Only the employees and agents of the Borough of West Chester are authorized to use the Borough's computer(s) or access the internet through the Local Area Network. No employee has the authority to permit others to use the Borough's computer(s) for any purpose without the prior approval of a department manager.
4. The use of **file sharing applications** or **peer to peer applications** over the internet is strictly prohibited on the Borough's network.
5. The use of the internet to access, download or display pornographic, obscene or otherwise offensive materials is strictly prohibited and will be considered a violation of the Borough's policies.
6. No information or materials related to Borough business or operations may be posted on the internet without prior approval.

7. The terms of the Agreement between the Borough of West Chester and the selected Internet Service Provider apply to all internet usage by Borough employees except that the Borough of West Chester makes no assurances of privacy as to any employee's usage of the Borough's computer(s) or the Internet through the Borough's computer network. The Borough of West Chester specifically retains the right to review employee's usage of the Borough's computer(s) and the Internet to assurance compliance with these policies.

8. The Borough of West Chester has a software solution in place that monitors all Internet traffic occurring over the Borough's computer network and has the obligation to investigate any report of misuse.

9. Any employee violating the computer usage policies may be subject to disciplinary action, up to and including discharge. In addition, the Borough of West Chester retains the right to discontinue the policy of permitting employee access to the Borough's computer(s) for non-Borough business, at any time.

Policies on eMail Usage

1. Only borough related business shall be transmitted and stored utilizing Borough computers on the network.

2. Employees shall only use software provided by the Borough of West Chester for sending, receiving and storing email and associated documents.

3. Sending, receiving or forwarding pornographic, obscene or otherwise offensive material through the Borough's computer network via the email server is strictly prohibited.

5. Sending or receiving files in excess of 10mb is prohibited unless approved by the information technology manager.

6. Borough email shall not be considered private and will be accessed by authorized personnel in the case of misuse investigation.

City of Pottstown

VOICE MAIL, ELECTRONIC MAIL AND INTERNET COMMUNICATIONS POLICY

Policy Statement

Voice mail, E-mail and usage of the Internet are considered by THE CITY to be important forms of corporate communication. All communications within our intra-office computer network or telephone network and sent or received through the Internet, including the contents of an employee's computer, are the property of THE CITY and should be for business purposes only. All communications should be professional in nature. The use of these systems for defamatory, obscene, sexually explicit, illegal, offensive, threatening or other inappropriate communications is strictly prohibited. Improper use of THE CITY computer resources or network and telephone resources or network is grounds for discipline up to and including discharge.

Monitoring and Control

THE CITY retains the right to monitor all Internet usage, voice mail, and E-mail messages during the ordinary course of its business without notice to the user, sender or recipient of the message, except as restricted by applicable law. For example, monitoring may be necessary to protect and ensure the system's security, to ensure that employees are not using voice mail or E-mail to communicate improper content, such as unlawful harassment, improper management techniques, unauthorized disclosure of confidential information and trade secrets, and to ensure that employees are not communicating to unauthorized recipients. THE CITY will actively monitor Internet usage, voice mail and E-mail communications, and reserves the right to inspect any and all files stored in private areas of our computer network or telephone network in order to ensure compliance with policy.

No Expectation of Privacy

Since all voice mail and E-mail messages are the property of THE CITY, we will monitor these communications to ensure that our computer and telephone systems are being used for legitimate business purposes only, and to protect THE CITY from liability. Employees and those communicating with employees must realize that they have no right or expectation of privacy in their voice mail or E-mail communications. All messages are subject to review by management, and all communications are subject to scrutiny, except as restricted by applicable law.

Permanency of Communications

Deleting voicemail or E-mail messages does not guarantee that they are erased from the system. Employees should not believe that privacy of voice mail or E-mail communications

is created by their efforts to delete incoming or outgoing messages. In addition, in the case of litigation, technology may exist to restore deleted voice mail or E-mail. Employees should be prepared to defend in court under oath the content of anything communicated in a voice mail or E-mail. Employees should not comment on issues that are in litigation or are capable of turning into litigation.

No Harassment

No voice mail or E-mail messages should be created or sent which might constitute intimidating, hostile or offensive material on the basis of sex, race, color, religion, national origin, age, sexual preference or disability. Harassment is broadly defined as anything which has improper (e.g. sexual) content and is both unwelcome and offensive to a reasonable person. The display of any kind of sexually explicit image or document in any CITY system is prohibited. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using THE CITY computer or telephone resources. Please refer to THE CITY policy against sexual harassment. (See page 5.)

Internet Usage and Outside Software

These same policies apply to the use of the Internet and the use of outside software. The Internet is to be used only for legitimate business purposes and communications, not for personal use. Employees are not permitted, without prior authorization, to establish web pages which suggest THE CITY affiliation or other authorization by THE CITY. Employees may access and use the Internet through THE CITY's system, computers, modems or lines only for specifically approved purposes. Any software or files downloaded via the Internet into THE CITY network become the property of THE CITY. Any such files or software may be used only in ways that are consistent with their licenses or copyrights. No employee may use THE CITY computer resources knowingly to download or distribute pirated or outside software or data. No outside software should be installed on any CITY computer, as such installations may violate licensing agreements or contaminate the entire computer system with a computer virus. THE CITY's Internet facilities and computer resources may not be used knowingly to violate in any material way the laws and regulations of the United States or any other nation, or the laws or regulations of any state, city, province or jurisdiction. All communications on the Internet to or from THE CITY's system or computers owned or operated by THE CITY are subject to monitoring except as prohibited by law, and to all of the CITY's standard policies.

Consequences of Misuse

Misuse of the Internet, or voice-mail or E-mail systems, including unauthorized communications to third parties through use of the Internet or through the use of THE CITY's intra-office voice mail or E-mail systems, or unauthorized disclosure of confidential business information through these systems, is grounds for disciplinary action up to and including termination/

Purpose

E-mail is a critical mechanism for business communications at the City of Williamsport. However, use of City of Williamsport's electronic mail systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of the City.

The objectives of this policy are to outline appropriate and inappropriate use of the City of Williamsport's e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

Scope

This policy applies to all e-mail systems and services owned by the City of Williamsport, all e-mail account users/holders at the City (both temporary and permanent), and all City e-mail records. It is meant as a minimum guideline. Department heads may implement further restrictions at their sole discretion.

Account Activation/Termination

E-mail access at the City of Williamsport is controlled through individual accounts and passwords. Each user of the City's e-mail system is required to read and sign a copy of this E-Mail Acceptable Use Policy prior to receiving an e-mail access account and password. It is the responsibility of the employee to protect the confidentiality of their account and password information.

Most employees of the City of Williamsport are entitled to an e-mail account. E-mail accounts will be granted to third party non-employees on a case-by-case basis. Possible non-employees that may be eligible for access include:

- Employees of a Staffing Agency.
- Interns.
- Volunteers.

Applications for these temporary accounts must be submitted in writing by the department head to information technology services. All terms, conditions, and restrictions governing e-mail use must be in a written and signed agreement.

E-mail access will be terminated when the employee or third party terminates their association with the City of Williamsport, unless other arrangements are made. The City is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

General Expectations of End Users

Important official communications are often delivered via e-mail. As a result, employees of the City of Williamsport with e-mail accounts are expected to check their e-mail in a consistent and timely manner so that they are aware of important City announcements and updates, as well as for fulfilling business- and role-oriented tasks.

E-mail users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to remove himself or herself from the list, and is responsible for doing so in the event that their current e-mail address changes.

E-mail users are also expected to comply with normal standards of professional and personal courtesy and conduct.

Appropriate Use

Individuals at the City of Williamsport are encouraged to use e-mail to further the goals and objectives of the City. The types of activities that are encouraged include:

- Communicating with fellow employees, business partners of the City, and clients within the context of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities.

Inappropriate Use

The City of Williamsport's e-mail systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual e-mail use will not interfere with others' use and enjoyment of the City's e-mail system and services. E-mail use will comply with all applicable laws, all City policies, and all City contracts.

The following activities are deemed inappropriate uses of the City of Williamsport's systems and services and are prohibited:

- Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Use of e-mail in any way that violates the City's policies, rules, or administrative orders, including, but not limited to the Sexual Harassment policy.
- Viewing, copying, altering, or deletion of e-mail accounts or files belonging to the City or another individual without authorized permission.
- Sending of unreasonably large e-mail attachments. The total size of an individual e-mail message sent (including attachment) should be 10 megabytes (MB) or less.
- Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.

- Excessive personal use of e-mail resources. The City of Williamsport allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. The City prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-City commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

Monitoring and Confidentiality

The e-mail systems and services used at the City of Williamsport are owned by the City, and are therefore its property. This gives the City of Williamsport the right to monitor any and all e-mail traffic passing through its e-mail system. While the City does not actively read end-user e-mail, e-mail messages may be inadvertently read by IT staff during the normal course of managing the e-mail system.

In addition, backup copies of e-mail messages may exist, despite end-user deletion, in compliance with the City's record retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss.

If the City discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify an employee if his or her e-mail records are to be reviewed. Notification may not be possible, however, if the employee cannot be contacted, as in the case of employee absence due to vacation.

Use extreme caution when communicating confidential or sensitive information via e-mail. All messages sent or received through the City of Williamsport's systems become the property of the City. Also keep in mind that all e-mail messages sent outside of the City's systems become the property of the receiver. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply" command during e-mail correspondence.

Reporting Misuse

Any allegations of misuse should be promptly reported to your department head. Your department head will then contact Information Technology Services. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the individual named above.

Disclaimer

The City of Williamsport assumes no liability for direct and/or indirect damages arising from the user's use of the City's e-mail system and services. Users are solely responsible for the content they disseminate. The City of Williamsport is not responsible for any third-party claim, demand, or damage arising out of use the City's e-mail systems or services.

Failure to Comply

Violations of this policy will be treated like other allegations of wrongdoing at the City of Williamsport. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use on the City’s e-mail systems and services may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of e-mail access;
2. Disciplinary action according to applicable City policies;
3. Termination of employment; and/or
4. Legal action according to applicable laws and contractual agreements.

Acknowledgement of Policy Acceptance

I hereby acknowledge that I have read and understand the E-mail Acceptable Use Policy. I agree to abide by this policy and ensure that persons working under my supervision abide by this policy. I understand that if I violate such rules, I may face legal or disciplinary action according to applicable laws or departmental policy.

Dept. Head: _____

Signature: _____

Date: _____

ORDINANCE NO. _____

AN ORDINANCE OF THE CITY OF READING, BERKS COUNTY, PENNSYLVANIA, AUTHORIZING THE CITY TO ENTER INTO AN INTERGOVERNMENTAL AGREEMENT FOR THE PURPOSE OF PROVIDING MUTUAL AID AMONG THE COUNTY OF BERKS, THE FRIENDSHIP HOOK AND LADDER COMPANY NO. 1 OF BOYERTOWN, PA, THE CITY OF READING AND THE TOWNSHIP OF SPRING TO ASSIST FIRST RESPONDERS IN THE MITIGATION OF EMERGENCIES RELATED TO TRENCH AND STRUCTURAL COLLAPSE

BE IT ENACTED and ORDAINED by the City Council of the City of Reading, Berks County, Pennsylvania and it is hereby enacted and ordained by the authority of the same as follows:

Section 1. Purpose. A mutual aid agreement between the County of Berks ("County"), The Friendship Hook and Ladder Company No. 1 of Boyertown, PA ("Fire Company"), the City of Reading ("City") and the Township of Spring ("Township") (collectively, the "Partners") to assist first responders in the mitigation of emergencies related to trench and structural collapse consistent with the requirements of the Pennsylvania Emergency Management Services Code and with the objectives of protecting the health, safety and welfare of municipal residents and landowners.

Section 2. Grant of Power. This Ordinance is adopted pursuant to authority granted in:

(A) The Pennsylvania Emergency Management Services Code, Act 323 of November 26, 1978 (35 Pa.C.S.A §7101, et seq.) as amended, or as it may be amended from time to time;

(B) The Pennsylvania Intergovernmental Cooperation Act, Act 177 of 1996 (53 Pa.C.S.A., Section 2301, et seq.) as amended, or as it may be amended from time to time.

Section 3. Definitions. The following words or phrases, when used in this Ordinance, shall have the meanings indicated:

Code - the Pennsylvania Emergency Management Services Code, Act 323 of 1978 (35 Pa.C.S.A. §7101, et seq.) as amended, or as it may be amended from time to time.

DES - the Berks County Department of Emergency Services, Berks County,

Pennsylvania.

Section 4. Participation. Pursuant to and in accord with the above-referenced authority, City is hereby authorized to participate with the County, Fire Company and Township in a mutual aid agreement for reciprocal emergency assistance regarding the ownership, possession, use and training for use of emergency equipment in accordance with the authority granted in the above-referenced laws and this Ordinance.

Section 5. Authority to Enter Agreement. Pursuant to and in accordance with the above-referenced authority, City is hereby authorized and directed to enter into the Reciprocal Agreement which governs the ownership, possession, use and training for use of emergency equipment, a copy of which is attached to this Ordinance and incorporated herein by reference (the "Agreement"). The Mayor is authorized to execute the Agreement on behalf of the City of Reading.

Section 6. Organization. The Agreement authorized under and by virtue of the authority of the Code and this Ordinance shall be between the County, Fire Company, Township and City. The participation by City in the Agreement shall be governed and controlled by the terms and conditions of the Agreement, as duly amended, the provisions of applicable Pennsylvania laws and regulations, and such other policies as may be duly adopted in accordance with the Agreement.

Section 7. Finances. Security and maintenance of the equipment shall be provided with funds provided by the Partners in accordance with the provisions of the Agreement referred to above, and such other grants or funding as may be available. The manner and extent of financing the Agreement shall be as follows: (i) no borrowing will be required by the City to fund its obligations under the Agreement; (ii) funds to implement the City's obligations under the Agreement shall come from usual budgeted amounts for such matters; and (iii) other provisions governing the manner and extent of financing joint projects and purchases shall be as set forth in the Agreement.

Section 8. Administration. The administration of the Agreement shall be undertaken in accordance with the terms of the Agreement.

Section 9. Term. The Agreement shall be for an indefinite term and dependent upon the continued participation of the Partners. The Partners can withdraw from the Agreement upon thirty (30) days prior written notice as provided for in the Agreement.

Section 10. Property. All property shall be acquired, managed, or disposed of pursuant to the Agreement in accordance with the terms of the Agreement and ownership of the Property shall remain with the County through DES. No acquisition of real property or real estate is authorized.

Section 11. Repealer. Any and all ordinances or parts of ordinances conflicting with the provisions of this Ordinance are hereby repealed insofar as they are inconsistent with this Ordinance's provision.

Section 12. Severability. If any article, section, subsection, provision, regulation, limitation, restriction, sentence, clause, phrase or word in this Ordinance, is, for any reason declared to be illegal, unconstitutional or invalid, by any Court of competent jurisdiction, this decision shall not affect or impair the validity of the Ordinance as a whole, or any other article, section, subsection, provision, regulation, limitation, restriction, sentence, clause, phrase, word, or remaining portion of the within Ordinance. The City Council of the City of Reading, Pennsylvania, hereby declares that it would have adopted the within Ordinance and each article, section, subsection, provision, regulation, limitation, restriction, sentence, clause, phrase and word thereof, irrespective of the limitations, restrictions, sentences, clauses, phrases, or word that may be declared illegal, unconstitutional or invalid.

Section 13. Code of Ordinances. The Code of Ordinances, as amended, of the City of Reading, Berks County, Pennsylvania shall be and remain unchanged and in full force and effect except as amended, supplemented, and modified by this Ordinance. This Ordinance shall become a part of this Code of Ordinances upon adoption.

Section 14. Effective Date. This Ordinance shall become effective in ten (10) days, in accordance with Charter Section 219.

Adopted _____, 2010

Council President

Attest:

City Clerk

Submitted to Mayor: _____

Date: _____

Received by the Mayor's Office: _____

Date: _____

Approved by Mayor: _____

Date: _____

Vetoed by Mayor: _____

Date: _____

EXHIBIT "A"
RECIPROCAL AGREEMENT