

CITY OF BRIDGEPORT

Subject: Computer, Internet and E-Mail Usage Policy			
---	--	--	--

PURPOSE

This policy establishes the acceptable use of electronic systems and tools provided by the City of Bridgeport, including but not limited to Computers, E-Mail and the Internet.

SCOPE

This policy shall apply to all City employees. The City reserves the right to amend this policy, and suspend or revoke the privileges bestowed herein.

POLICY

The City of Bridgeport provides access to the vast information resources of the Internet to help City employees in the performance of their jobs. The facilities to provide access represent a considerable commitment of city resources for telecommunications, networking, software, storage, etc. This policy is designed to advise the employee of the City's expectations for the use of those resources, **and to help the employee use these resources wisely.**

The employee is expected to use the **Computers**, Internet and E-Mail for business-related purposes, to research relevant topics and obtain useful business information. Personal use of the Computers, Internet or E-Mail during normal working hours shall be limited so as not to interfere with appropriate work efforts. Department supervisors are **expected** to monitor personal use of the **Computers**, Internet and E-Mail, and discourage excessive use. The City expects that employees using the **Computers**, Internet, and E-Mail will conduct themselves honestly and appropriately, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others. All existing City policies apply to the employee's conduct on the **Computer**, Internet and the use of E-Mail, including but not limited to, those that deal with intellectual property protection, privacy, misuse of City resources, sexual harassment, information and data security, and confidentiality.

The chats, news groups and email of the Internet gives each user an immense and unprecedented reach to propagate the City's message. Employees must take special care to maintain the clarity, consistency and integrity of the City's posture. Therefore, each employee is expected to forgo a measure of his individual freedom when participating in chats or news groups on City business, as outlined below.

While the City's connection to the Internet offers a plenitude of potential benefits, it can also expose the City to significant risks if employees do not follow appropriate security protocol. As detailed below, this may require preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features, i.e. file transfers. The overriding principle is that security is to be the employee's first concern. An Internet user can be held accountable for any breaches of security or confidentiality.

DEFINITIONS:

Certain terms in this policy should be understood expansively to include related concepts.

City of Bridgeport – includes all City departments, related agencies and all staff (full, part time, **temp**, etc.) working for them.

Display – includes monitors, flat-panel active or passive matrix displays, monochrome LCDs, projectors, televisions and virtual-related tools.

Document – covers any kind of file that can be read on a computer screen as if it were a printed page, including the HTML files read in an Internet browser, any file meant to be accessed by a word processing or desk-top publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools.

E-Mail – refers to any and all electronic mail sent or received utilizing the City of Bridgeport Personal Computer network or it's Internet connection.

Graphics – includes photographs, pictures, animations, movies or drawings.

Internet – refers to any world wide computer network connecting thousands of computers and millions of individual world wide subscribers.

Obscene materials – material is obscene if taken as a whole, it is offensive, depicts or describes in a patently offensive way any sexual act, and if taken as a whole, it lacks serious literary, artistic, educational, political or scientific value.

Sexually explicit – material that graphically depicts or describes sexual conduct, including but not limited to, sexual intercourse, and which lacks educational or scientific value.

City's facilities – **Anything pertaining to Computers, Internet, and E-Mail.**

USAGE REGULATIONS AND PROCEDURES

1. Files, E-Mail, documents and other electronically stored material on the City's network and computers are not private. The City has software and systems in place that can monitor and record all Internet and E-Mail usage. The employee must be aware that the City's security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, news group, or E-Mail message, and each file transfer into and out of our internal networks, and the City reserves the right to do so at any time. No employee should have any expectation of privacy in his or her Internet or E-Mail usage. The ITS department will review Internet and e-mail activity and analyze usage patterns, and City management may choose to publicize this data to assure that the City Internet and E-Mail resources are devoted to maintaining the highest level of productivity.
2. The City reserves the right to inspect any and all equipment, file(s), and E-Mail stored in private areas of our network, **or on any Computer**, in order to assure compliance with City policy or in the normal course of business. Reasons for inspection or review include, but are not limited to: system, hardware or software problem, suspicion of crime or the need to perform work or provide service when an employee is not available.
3. **The City reserves the right to remove any files or software which is not approved by the ITS Dept, and/or inform Department's Managers of the situation.**
4. The City's network uses independently supplied software and data to identify inappropriate, obscene or sexually explicit Internet sites. The City may block access from within our networks to all such sites that we know of. If you find yourself connected **inadvertently** to a site that contains sexually explicit or obscene material, you must disconnect from that site immediately, regardless of whether that site has been deemed acceptable by any screening or rating program. An employee, who is denied access to any such site, should **contact their respective Department's Manager** if the information and data contained therein are required for work related reasons.
5. Any files or software downloaded via the Internet into the City network becomes the property of the City, and **must be pre-approved by the ITS Dept**, and used only in ways that are consistent with their licenses or copyrights.

6. The City retains the copyright to any material posted to any forum, news group, and chat or World Wide Web page by any employee in the course of his or her duties.
7. The City will comply with reasonable requests from law enforcement regulatory agencies for logs, diaries and archives on individual's Internet and e-mail activities.

EMPLOYEE'S RESPONSIBILITIES

The City's Internet facilities, computing resources, **and software installed by ITS**, shall not be used in an unacceptable manner. It is the employee's responsibilities to familiarize himself/herself with this policy, so as to ensure compliance.

1. The City's Internet facilities and computing resources, including all E-Mail, must not be knowingly used to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city province or other local jurisdiction in any material way. **Use of City resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.**
2. The display of any kind of obscene or sexually explicit image or document, as defined above, on a City system is a violation of our policy on sexual harassment. In addition, obscene or sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.
3. No employee may use City facilities knowingly to download or distribute pirated software or data.
4. No employee shall use City facilities to knowingly create, send, forward, download, print or store messages or graphic images which are harassing, threatening, intimidating, libelous, slanderous, or discriminatory or defamatory in nature.
5. No employee may use the City's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
6. No employee may use the City's Internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
7. Each employee using the Internet facilities shall identify himself or herself honestly, accurately and completely (including one's city affiliation and function where requested). An employee who releases their personal information, including personal identifying information, does so at their own risk.
8. Employees are reminded that chats and news groups are public forums where it is inappropriate to reveal confidential City information, customer data, trade secrets, and any other material covered by existing City secrecy policies and procedures. Employees releasing protected information via a news group or chat, whether or not, the release is inadvertent will be subject to all penalties under existing security policies and procedures.
9. Use of City Internet access facilities to commit infractions such as misuse of City assets or resources, sexual harassment, discrimination, unauthorized public speaking, or misappropriation or theft of intellectual property are also prohibited by general City policy, and will be sanctioned under the relevant provisions of that policy and any applicable state and federal laws.
10. Since a wide variety of materials may be deemed offensive by colleagues, customers or suppliers, it is a violation of City policy to store, view, print, or redistribute any document or graphic file that is not directly related to the user's job or the City's business activities.
11. Employees with Internet access may not use City Internet facilities to download entertainment software or games, or to play games against opponents over the Internet. Employees should also avoid using their personal software to play games, create inappropriate screen savers, etc.
12. Employees with Internet access may not upload any software licensed to the City or licensed by the City without explicit authorization from the ITS Department.
13. Employees may not intentionally intercept, record, alter or receive another employee's E-Mail. In addition, employees shall not send E-Mail messages using another employee's I.D. or access the Internet at another employee's computer.
14. No employee shall use the City of Bridgeport Personal Computer network or Internet E-Mail facilities for advertisement **or conducting of business for profit**, to distribute or advertise materials not related to City business or use the facilities for frivolous messages.
15. **The City's employees shall not subscribe to non-business related E-Mail such as jokes/pictures/horoscope/prayer of the day, etc. The distribution of chain letters is forbidden.**

16. **No software may be installed or downloaded unless pre-approved and performed by ITS.**

TECHNICAL PROCEDURES

1. User IDs and passwords help maintain individual accountability for **Computer, Internet and E-Mail** resource usage. Any employee who obtains a password or ID for an Internet resource must keep that password confidential. **City policy prohibits the sharing of user IDs or passwords.**
2. Any file that is downloaded must be scanned for viruses before it is run or accessed.

SECURITY

1. The ITS Department has installed a variety of firewalls, proxies, Internet address screening programs and other security systems to assure the safety and security of the City's networks. Any employee who attempts to disable, defeat or circumvent any City network security facility will be subject to discipline, up to and including, immediate dismissal.
2. Files containing sensitive company data as defined by existing federal, state and city data security policies that are transferred in any way across the Internet must be encrypted.
3. City computers that use their own modems to create independent data connections sidestep our security mechanisms. An individual City computer's private connection to any outside computer that is **authorized by ITS** for use for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from the City's internal network.
4. Only those Internet services and functions with documented business purposes for the City will be enabled to the Internet firewall.
5. Because unscrupulous or malevolent Web sites operators can take control of an unsuspecting visitor's computer using apparently routine JAVA or file transfer operations, such transactions can introduce material risks to network security for which there is no bullet-proof technical solution short of complete abstinence. City network security policy requires that all FTP transactions and JAVA downloads be blocked at the [*outermost*] firewall.

VIOLATIONS

Violations of this policy will be reviewed on a case by case basis, and can result in disciplinary action, up to and including, suspension and termination. Any known or suspected violation of this policy shall be reported to the employee's immediate supervisor and/or department head.

ACKNOWLEDGMENT

I acknowledge that I have received a written copy of the Computer Internet and E-Mail Usage Policy for the City of Bridgeport. I understand the terms of this policy and agree to abide by them. I realize the City of Bridgeport 's security software may record and store for management use the electronic E-Mail messages I send and receive, the Internet address of any site that I visit, and any computer network activity in which I transmit or receive any type of data. I understand that any violation of this policy could lead to my dismissal from employment or even criminal prosecution.

Internet access approval by Department Head

Approved_____ Disapproved_____

Department Head Name (Print) Department Head Signature Date

Employee Name (Print) Employee Signature Date