Cambridge Police Department	**POLICY & PROCEDURES**	**No. 212**
	Subject/Title: **Internet, E-Mail, & Computer Usage**	
	Issuing Authority: Robert C. Haas, Police Commissioner	**Issue Date:** January 8, 2010 **Effective Date:** January 22, 2010 **Review Date:** **Rescinds:**
References/ Attachments: City of Cambridge's *"Internet and On-Line Computer Services Use Policy" (rev. 8/25/09)*	**Accreditation Standards:** 11.4.4; 82.1.6; & 82.1.7	

I. PURPOSE:

The purpose of this policy and set of procedures is to outline the standards under which members of this department may access and utilize the City of Cambridge and the police department's Internet, e-mail, other electronic systems, and associated equipment. This policy is also designed to achieve the following safeguards and protections as it relates to these networks and systems:

- Protect the City, the police department and its members from potential legal liabilities;
- Ensure the effective and efficient functions and operations of the police department;
- Prevent disruption caused by computer viruses, spyware, malware; outside interferences, etc.;
- Safeguard confidential and sensitive information;
- Increase employees' awareness of legal, security, and productivity issues relating to the use e-mail, the Internet, and other forms of instant messaging or social network services;
- Inform employees about how they may and may not use the police department's Internet, e-mail, and other electronic systems; and
- Comply with the City's policy on *"Internet and On-Line Computer Services Use."*[1]

[1] All members of the Cambridge Police Department are not only bound by this directive, but are also responsible for the compliance of the City of Cambridge's ***"Internet and On-Line Computer Services Use Policy"*** (see attached).

II. POLICY STATEMENT:

The use of the City of Cambridge and police department's automation systems, including computers, fax machines, and all forms of Internet/Intranet access, is for the police department's business and for authorized purposes only. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense to the City of Cambridge or the police department.[2]

Use of the City and police department's computers, networks, and Internet/Intranet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate work-related purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);
- Misrepresenting oneself or the police department;
- Violating the laws and regulations of the United States, Massachusetts General Laws, City of Cambridge Municipal Code, or any other nation or any state, city, or other local jurisdiction in any way;
- Engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the City or police department's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics;
- Causing congestion, disruption, disablement, alteration, or impairment of the City or police department's networks or systems;
- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;

[2] With the exception of those activities that have been identified in **Section VII. C.** of this directive.

- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Using recreational games; and/or
- Defeating or attempting to defeat security restrictions on company systems and applications.

III. GENERAL CONSIDERATIONS AND GUIDELINES:

The City of Cambridge and the Cambridge Police Department utilizes computers, computers systems, Internet access, as well as, other on-line services to facilitate and aid members of this department to accomplish its primary mission: responding to calls for services; preventing crime; investigations, detecting and apprehending criminals; and documenting incidents. Access to these systems and other databases, to include the Internet and e-mail services, are designed to make its members more effective and efficient in terms of timely and accurate response to the public.

With the use of computers as a communications tool, what took days or weeks to do a few years ago can now be done in minutes. Email, live-scan fingerprinting, digitized images, audio and video data can be transmitted to employees so as to further the level of communications and achieving the department's primary mission.

This technological advantage does not come without its own pitfalls and potential vulnerabilities. Misplaced media may result in the loss of a high volume of confidential data. A confidential image, casually forwarded, could end up in the electronic mail boxes of thousands of recipients or displayed on internet entertainment websites. Hackers may enter systems and access, change or destroy data. Viruses can enter the system via innocent files such as internet images and games, and wreak havoc on system operability, steal data or passwords, or allow unauthorized intruders to access the system.

This policy will serve as a guide to help all employees preserve the integrity of the department's data, manage use of computer systems, decrease liability exposure, and prevent unlawful or wrongful actions involving computers and data.

The policy supplements the policies and user agreements of state and federal data providers such as the CJIS network and other contracted databases.[3]

The City of Cambridge owns the rights to all data and files in any computer, network, or other information system used in the police department. The City of Cambridge and the police department also reserve the right to monitor electronic mail messages (including

[3] Refer to department policy entitled, ***#412 – Mobile Data Terminals & Handheld Devices***

personal/private/instant messaging systems) and their content, as well as any and all use of the Internet and of computer equipment used to create, view, or access e-mail and Internet content. Employees must be aware that the electronic mail messages sent and received using the City and police department's equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by City and police department officials at all times. The City and the police department have the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with policy and state and federal laws. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate City or police department official.

The City and/or police department have licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software.

IV. DEFINITIONS:

A. **Records Management Systems (RMS):** Refers to the system whereby all of the department's digital records are stored and maintained, such as, police reports, Master Name Index files, other department developed software systems to track information, etc.

B. **Software:** The programs, applications, data, routines, and operating information used within a computer.

C. **Hardware:** The tangible components of a computer such as disk drives, storage devices, monitors, keyboards, mouse, and other peripherals.

D. **Offensive/Disruptive Communications:** Communications which contain sexual content or sexual implications, racial slurs, gender-specific comments, or any other that offensively addresses a person's race, creed, religion, physical or mental disability, color, sex, national origin, age, occupation, marital status, political opinion, sexual orientation, or any other group status.

E. **Excessive:** For purposes of this directive, the use of the word "excessive" is construed to mean any utilization of the Internet, E-mail, or any other utilization

of electronic systems that interferes with normal job functions, responsiveness, or the ability to perform daily job activities.

F. **Material:** For purposes of this directive, the word "Material" is defined as any visual, textual, or auditory entity.

G. **Password:** A word or string of alpha-numeric characters used to restrict access to an account, network, database, or file to an authorized member.

H. **Virus:** A hidden code embedded within a computer program or file that is intended to corrupt a system or destroy data stored in a computer system.

I. **Malware:** Malicious computer software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the Internet.

J. **Spyware:** Is a type of malware that is installed on computers and collects information about users without their knowledge. The presence of spyware is typically hidden from the user. Typically, spyware is secretly installed on the user's personal computer.

K. **Systems Manager:** An individual assigned or authorized by and under the direction of the Police Commissioner to oversee and/or manage the operation and security of the department computer system and network.

V. PROCEDURES FOR SAFEGUARDING SYSTEMS & NETWORKS:

A. **Authorized Users:** The responsibility of protecting the hardware, software, and data from abuse is shared by all users of the department's data processing systems. The potential for someone (citizen or employee) to suffer a loss or inconvenience due to improper or inappropriate use of the department's data processing systems is real, whether malicious or accidental.

1. Only authorized users may have access to the department computer system. Authorized users shall have an individual user account provided by the Systems Manager.

a. Members of the department are not to share their usernames and passwords with any other person. No member of the department is to use the username or password of another at any time, nor will he/she access or transmit any information while logged into another person's username and password.

b. No member of the department will use the username or password of another. If a member of the department finds a computer already logged into one of the department's system, he/she will first log-off the user, prior to signing back into the system with his/her own username or password.

2. The use of department computer systems and equipment is solely for the purposes authorized by the department. Unauthorized use is a violation of this policy and set of procedures. In addition to the prohibited uses specified with the City's ***"Internet and On-Line Computer Services Use Policy"*** (revised August 25, 2009), the following uses of the department's electronic systems and network, will include the following:

a. Electronic communication should not be used to solicit or sell products or services that are unrelated to the City's or department's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

b. Using City and department's automation systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. Such material violates the City and police department's anti-harassment policies.

c. The City and department's electronic mail system, Internet access, and computer systems must not be used to violate the laws and regulations of the United States or any other nation or any state, city, or other local jurisdiction in any way. Use of department's resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. The department will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

d. Unless specifically granted in this policy, any non-business use of the department's automation systems is expressly forbidden.

B. Software Applications and Programs: All software programs installed or introduced onto the department's computers must be authorized by the Systems Manager. Software used in the department's computer systems is the property of the department and will not be used, copied or distributed without permission of

the Systems Manager. Members of the department are not permitted to introduce any unauthorized software, to include the following situations:[4]

a. Members are strictly prohibited from installing software programs which have not been authorized for use by the Systems Manager. Any unauthorized software, such as games and other personal amusement software, will be deleted.

b. No employee shall install or use software on department computers that is unlicensed, in violation of the software licensing agreement, or has been copied in violation of the law.

c. No employee shall introduce unauthorized programs or manipulate or alter programs running on mobile network computers, handheld devices, or desktop computers.

C. Data Files: Employees must use caution when introducing data files into department work stations. To this end, all employees are to observe and adhere to the following safeguards:

1. Data should be downloaded or received only from a trusted source.

2. Opening of suspect files for investigatory purposes should be done on designated investigative work stations only. The work stations are not connected to the department network.

3. All disks and external storage devices, including disk drives (i.e., thumb drives), will be scanned by the user for viruses when introduced into any department computer. This can be accomplished by right-clicking on the appropriate drive letter in the "My Computer" menu and choosing the option "Scan for Viruses" on the drop-down menu.

4. Employees shall not introduce unauthorized data files into mobile network computers, handheld devices or desktop computers from any source including CDs, DVDs, Thumb drives, other storage devices (i.e., external storage devices) or any other media or on-line sources.[5]

5. Employees shall not encrypt data, or change permissions or files, without the formal approval of the Police Commissioner or the Systems Manager.

[4] CALEA Std.: **11.4.4** – *A written directive establishes a policy for the introduction of computer software and data disks into agency-controlled computer systems hardware.*
[5] CALEA Std.: **11.4.4**

D. Use of Personal Electronic Equipment: The department prohibits the use or possession of certain types of personal electronic equipment in the workplace. Further, the department prohibits using personal electronic equipment, whereby images, digital records or recordings, and other forms of electronic information may be gathered and then used for personal purposes. Recognizing that personnel do have electronic devices, namely personal mobile phones which have a variety of capabilities, there may be certain applications they may use as long as it is in used in the furtherance of official duties, or as allowed by this and other policies.

1. Employees should not bring personal computers to the workplace or connect them to department's electronic systems unless expressly permitted to do so by the Police Commissioner, Division Commander, or Senior Commanding Officer in consultation with the Systems Manager. Any employee bringing a personal computing device or image recording device onto the department's premises thereby gives permission to the department to inspect the personal computer or image recording device at any time with personnel of the department's choosing and to analyze any files, other data, or data storage media that may be within or connectable to the personal computer or image recording device in question. Employees who do not wish such inspections to be done on their personal computers or imaging devices should not bring such items to work at all.

2. Employees who do capture images or record activities on their own personal electronic devices while in the performance of their official duties are not permitted to convert those electronic images or recordings for their own personal use. The department recognizes that such capabilities may serve as a valuable aid in the performance of their duties, whether it is in the furtherance of an investigation or some other police related activity, and therefore nothing in this policy should be construed to mean that members of the department cannot be used for such purposes.

    a. Any images or other recordings that are captured on a personal electronic device that has been captured for investigative purpose or that has evidential value should be handled and treated in accordance with department policy.

VI. USE OF E-MAIL SYSTEM:

A. General Guidelines for E-mail: The department's email system is intended for the use by its employees as an essential means of conducting the department's official business and has replaced most of the paper exchange that normally took place through the transfer of paper memoranda, convenience of orders, briefing memoranda on a variety of police matters, transmissions of department's official notices, and so on. So as to provide for an effective means of intradepartmental communications, the following protocols will always be observed:

1. All department personnel will be trained in the use of the email system(s). This training shall include how to access email, create email messages, open attachments, attach a document, send and receive email and manage an email account.

2. It shall be the responsibility of each employee to check the department's email system at least once per working shift and to read all e-mail messages, and associated attachments, received from department personnel.

3. Written directives may be distributed to employees by email. Once the mail is opened, it shall be understood that the directive has been formally issued to the officer and/or employee. The email receipt indicating that the employee received and opened the email shall serve as a record that the employee received and reviewed the written directive. For further information, refer to the department policy entitled, ***#110 – Written Directive System***.

4. Any email that is time stamped-delivered but has no date/time as to when it was opened shall be considered unread. If the message has no opened date/time and it does not exist in the recipient's mailbox, then it is considered to have been deleted, without being read by the recipient.

5. No member of this department should delete any department related email without first opening it and reading the email and/or its attachments.

6. The emails of the department employees are considered public record, unless the content falls under a statutory exemption.[6] It is unlikely that emails containing jokes, obscene images, or personal comments to others will fall under one of the statutory exemptions.

7. The following types of email activities are expressly prohibited:

   a. Transmission of global or mass mailings unless related to department business or unless prior authorization has been received from the Police Commissioner, Superintendent, or Deputy Superintendent.

   b. Transmission of chain letters or virus alerts.

   c. Transmission of any email containing abusive, harassing, discriminatory, or sexually explicit language or content.

[6] M.G.L. c. 4, § 7

d. Transmission of deceptively labeled emails, to include any emails containing a misleading subject line, is anonymous, is attributed to another person, or identifies its true sender incorrectly.

e. Inclusion of Criminal Offender Record Information (CORI) within any email, except where the recipient's email address has been previously confirmed to be a legitimate and secure reception point.

f. Any other transmissions or inclusions that violate federal, state, or local law.

B. Confidentiality of Electronic Mail: As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable state and federal laws, and City's and department's rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

It is a violation of department's policy for any employee, including Systems administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others. Employees found to have engaged in such activities will be subject to disciplinary action.

Electronic Mail Tampering: Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

VII. INTERNET/INTRANET NETWORKS:

A. Access to Internet/Intranet Networks: The Internet is to be used to further the department's mission, to provide effective service, work-related research, and to allow employees to perform legitimate business purposes only. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are City's and police department's resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal

use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

B. **Employee Liability for Inappropriate Use:** Employees may be personally liable both for applicable criminal and/or civil violations of the law as it relates to any and all damages incurred as a result of violating department's security policy, copyright, and licensing agreements. This liability extends to the following activities:

1. All City of Cambridge and police department's policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, company information dissemination, standards of conduct, misuse of company resources, anti-harassment, and information and data security.

2. Users shall not use the department system to access, download, upload, store, print, post, or distribute pornographic, obscene, or sexually explicit materials.

3. Users may not visit an otherwise unacceptable site unless it is for a specific legitimate law enforcement investigation and only with the approval and authorization of a supervisory officer.

4. If an employee accidentally accesses an unacceptable site, the employee must immediately disclose the incident to a supervisor. Such disclosure may serve as a defense against an accusation of an intentional violation of this policy.

C. **Strictly Prohibited Activity:** Use of the department's Internet/Intranet network for Instant messaging software and other forms of social network services (i.e., Facebook, Twitter, MySpace, LinkedIn, blogging, etc.), movies, music sharing software or other peer-to-peer data software are prohibited activities at all times.[7] Further, employees may not engage in any form of personal business while working, or through the use of the department's Internet/Intranet networks.

D. **Release of Department Records:**[8] Records, including records containing criminal history data, may be released only in accordance with department policy.[9] Data maintained or obtained by this department shall not be distributed in violation of investigative confidentiality or CORI through email, or uploading

[7] This provision of the policy does not pertain to those situations when an officer is engaging in such activity strictly for a specific legitimate law enforcement investigation and only with the approval and authorization of a supervisory officer.
[8] CALEA Std.: **82.1.7**
[9] Refer to department policy entitled, ***#360??? – Criminal Justice Information System.***

to chat (Officer.com) or entertainment sites (i.e., Break.com, Rotten.com, etc.). Data may be distributed for legitimate law enforcement purposes only and in accordance with established protocols.