

Rev. August 25, 2009

## City of Cambridge Internet and On-line Computer Services Use Policy

### Overview

The City of Cambridge's computer networks are connected to the Internet and other on-line services in order to allow City government to serve the public more efficiently and effectively. Accordingly, various on-line capabilities are made available to designated City employees for legitimate, work-related purposes. These capabilities may include the ability to send and receive electronic mail (E-mail), to conduct research and financial transactions on the Internet, to gain access to computers not owned or controlled by the City, and to copy data to and from remote computer sites.

Use of these capabilities is subject to the same management oversight and supervision as any other employee activity. Such use must conform to all applicable laws and regulations. All official policies and procedures established by the City Manager or his designees to regulate the behavior and performance of City employees shall apply to use of these computer capabilities. Failure to comply with the guidelines in this policy may result in termination, suspension, or other limitation of an employee's privileges for access to Internet-related capabilities, and may be the cause for further discipline up to and including discharge.

### Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the City of Cambridge. These rules are in place to protect the employee and the City of Cambridge. Inappropriate use exposes the City to risks including virus attacks, compromise of network systems and services, loss of productivity and legal issues.

### Scope

The policy applies to City employees, contractors, consultants, temporaries, and other workers at the City of Cambridge, including all personnel affiliated with third parties. This policy applies to all equipment, PC, peripherals, Software & Network applications and any other equipment or media related to computer usage.

These regulations may be updated from time to time and amended at the discretion of the City Manager.

### Policy

#### 1. General Use and Ownership

- a. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If issues arise not covered by this policy then users should consult Department Heads or Supervisors for guidance.
- b. All City owned computer and network equipment is provided for the purpose of conducting City business.
- c. Managers and supervisors are responsible for ensuring that all their employees using computers have read this Policy and understand its applicability to their activities.
- d. The City Manager may, for legitimate business reasons, approve the monitoring of e-mail messages. Legitimate business reasons includes, but is not limited to, system checks, review of employee productivity when employee productivity is called into question by a supervisor or manager, investigations into claims of possible criminal activity, and investigations into claims of inappropriate use of the City's internet or on-line services.

- e. Use of the City's system constitutes consent to monitoring of e-mail transmissions and other on-line services and is conditioned upon strict adherence to this Policy.
- f. E-mail and other on-line services are the property of the City of Cambridge, and should be used for business purposes.
- g. E-mail messages are considered public records and are therefore legally discoverable and subject to record retention policies. Employees should not expect that e-mail messages (even those marked "personal") are private or confidential.

## **2. Unacceptable Use**

### ***The following activities are strictly prohibited:***

#### ***System and network activities:***

- a. Any illegal activity, including, but not limited to, the transmission of copyright or trade secret material, the transmission of obscene or threatening material, or the participation in any type of criminal or terrorist activity.
- b. The transmission of materials used for commercial promotion, product endorsement, or political lobbying.
- c. Attempts to violate the computer security systems implemented by the City of Cambridge ITD Department or other institutions, organizations, companies, or individuals. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- d. All users are expected to undertake precautions to prevent infection of City computers by computer viruses. In particular, executable programs imported from other sites to City computers must not be used unless they have been authorized by the Information Technology Department (ITD) and they have been subjected to virus detection procedures approved by ITD. The IT Department may, from time to time, impose additional restrictions or regulations on the importing of remote files, and such restrictions or regulations shall be considered part of this Policy.
- e. Political lobbying or other activities that may be deemed to be political in nature shall be permitted to the extent that such activities are a part of the official responsibilities of an employee, provided that such activities relate to political issues rather than to specific political candidates.
- f. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which The City of Cambridge or the end user does not have an active license is strictly prohibited.
- g. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed every 90 days or when prompted by the IT Department.

- h. Providing information about, or lists of, City employees to parties outside of the City of Cambridge without supervisor or manager authorization.
- i. All employees and representatives are prohibited from accessing any streaming media programs, feeds, material and content unless the subject matter being streamed is necessary to fulfill one's job responsibilities. No streaming media sites are to be accessed, nor are any streaming media programs or applications to be downloaded, installed and/or operated by end users using City computers, servers, systems and/or networks unless the material is necessary to fulfill one's job responsibilities.
- j. Employees are also prohibited from accessing media streams from such Web sites as YouTube, Hulu, FaceBook, and MySpace, among others, unless the subject matter being streamed is necessary to fulfill one's job responsibilities.

### ***Email and Communications Activities***

- a. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- b. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- c. Unauthorized use, or forging, of email header information.
- d. Participating in the viewing or exchange of pornography or obscene materials.
- e. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- f. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- g. Use of unsolicited email originating from within City of Cambridge's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by The City of Cambridge or connected via the City's network.
- h. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups

### ***Blogging***

- a. Blogging by employees, whether using City of Cambridge's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of City systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the City's policy, is not detrimental to City of Cambridge's best interests, and does not interfere with an employee's regular work duties. Blogging from City of Cambridge's systems is also subject to monitoring.
- b. City of Cambridge's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, when engaged in blogging.
- c. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of City of Cambridge and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by City of Cambridge's Non-Discrimination and Anti-Harassment policy.

- d. Employees may also not attribute personal statements, opinions or beliefs to City of Cambridge when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of City of Cambridge. Employees assume any and all risk associated with blogging. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, City of Cambridge's trademarks, logos and any other City of Cambridge intellectual property may also not be used in connection with any blogging activity.