Luke A. Bronin
Mayor

POLICY NO: **010**

DATE: **February 1, 2018**
DISTRIBUTION: **Affected Personnel**
SUBJECT: **Acceptable Use Policy of Information Technology (IT) Resources**

I. PURPOSE:

The purpose of this memorandum is to establish the City's policy regarding acceptable use of information technology (IT) resources, including the use of computers, electronic mail ("E-mail") and the Internet connection. Included also are the City's policies for maintaining the security of City's network servers and personal computers, and ensuring compliance with software licenses and applicable copyright laws.

II. RESPONSIBILITY:

It shall be the responsibility of all City personnel, contractors, interns, or guests to comply with these provisions while using any of the City's information technology resources, including computer, Internet and email access. Usage must be in accordance with applicable City policies that govern all forms of communication and expression and applicable state and federal laws and collective bargaining agreements.

III. DEFINITIONS:

i. Information Technology Resources

As used in this document, the term "information technology resources" refers to all of the City's information technology systems and components. These include, but are not limited to, the voice and data network, the Internet connection, personal computers, printers, servers, access to research databases and services, other communications equipment such as cellular telephones and smart phones, or peripherals, software programs and data leased, owned, maintained and/or operated by the City.

ii. User

As used in this document, the term "user" refers to employees, contractors, students, interns, volunteers, and guests or other authorized users of the City.

iii. MetroHartford Innovation Services (MHIS)

Metro Hartford Innovation Services (MHIS) is the information technology organization for the City of Hartford and the Hartford Public Schools, as established in Hartford Municipal Code Chapter 2, Article IV §2-105. As such, MHIS has authority over matters of technology systems, infrastructure, and installation. MHIS's authority is vested in the Chief Information Officer and his/her designees.

iv. Code of Ethics or Ethics Code

Hartford's Code of Ethics for its officers, officials and employees appears in Chapter 2, Article XIX §2-900 et seq of the Hartford Municipal Code and is referred to herein as the Code of Ethics or the Ethics Code.

v. Use of social media services (e.g. Flickr™, Twitter™ and Facebook™) is regulated by, and must comply with, the City's Social Media Policy.

vi. All trademarks referenced in this policy are the properties of their respective owners.

IV. IT IS THE POLICY OF THE CITY OF HARTFORD, THAT:

i. Employees shall exercise caution and care in using, transporting, securing, and otherwise handling office-owned computers and software.

    i. Laptops are particularly subject to damage and theft and employees traveling with a laptop shall take all reasonable precautions to prevent damage and theft of the laptop. Report any loss or theft to your Department Head and MHIS as soon as possible. Users must also exercise reasonable precautions in order to prevent the introduction of a computer viruses or other malicious programs into the network.

ii. Each employee shall be provided with the tools to do his or her work, including a computer and appropriate software.

    i. The City will only do so in compliance with all of its vendors' licenses and applicable copyright laws. Computer programs are intellectual property and software publishers license their programs to protect their property rights from infringement. In addition, legal protections can also exist for any information published on the Internet. The City respects the rights of intellectual property owners.

iii. No user shall download or install software from the Internet or any other source or save software attached to email messages to their workstation or network file share without the prior written approval of the Chief Information Officer.

i. The use of software from unauthorized sources may also present security threats or interfere with the functionality of the network and such software will not be installed or used on City computers

iv. No user should have any expectation of privacy while using City information technology resources. As such, the City retains the right to inspect any user's computer or mobile device and the files contained therein.

i. The firewall between the Internet and the network automatically checks all data moving between the network and the Internet, identifying the sending and receiving systems stations. Individual workstation activity is logged and users should assume that any files they create or receive, any messages they send or receive, and any web sites that they visit are subject to monitoring.

v. All incoming, outgoing and internal calls are logged. The logging captures calling station, called station, and duration of call.

vi. The Chief Information Officer or her/his designee may make assessments of software use, announced and unannounced audits of City computers, and take any other actions considered necessary to assure compliance with this policy. The Chief Information Officer or her/his designee shall remove from any computer any unauthorized software found for which a valid license or proof of purchase is not available

vii. It is unacceptable for any employee, contractor, student, intern, volunteer, guest or other authorized user to use any of the City's Information Technology Resources:

i. in the furtherance of any illegal act, including violations of any federal or state laws or

ii. regulations;

iii. for any political purpose;

iv. for any commercial purpose;

v. to infringe on any intellectual property rights;

vi. to send threatening or harassing messages;

vii. to libel or otherwise defame any person;

viii. to access or share sexually explicit materials;

ix. to distribute chain letters;

x. to intercept communications intended for other persons;

xi. to gain, or attempt to gain, unauthorized access to any computers or networks;

xii. for any use that causes interference with, or disruption of, network users and resources,

xiii. including, but not limited to, propagation of computer viruses or other harmful programs;

xiv. to misrepresent either the City or a person's role in the City;

xv. to access and/or share personal identifiable information; or

xvi. in any manner that is prohibited by this policy or any other policy of the City, or in any unprofessional manner.

xvii. the list of activities is not intended to be exhaustive and all questions regarding licenses, copyright laws, or appropriate use should be addressed to the Chief Information Officer.

viii. The City reserves the right to block access to any web site or on-line service. Use of "anonymizing" or "proxy" web sites to circumvent filtering and access controls is strictly prohibited. Management reserves the right to audit, inspect, examine or track any user's use of the Internet.

ix. Harassment of any kind is prohibited. Messages with derogatory or inflammatory remarks about an individual or group's race, color, religious creed, age, sex, marital status, national origin, ancestry, disability, or sexual orientation will not be tolerated.

x. Users may utilize the Internet in pursuit of job-related professional or educational development, research and analysis activities.

xi. Users may utilize the Internet connection or email system for personal, non-business use.

i. Such use should be brief and incidental; should otherwise be consistent with this policy; and must not interfere with a user's prescribed duties and responsibilities

ii. Pursuant to section §2-902(B) of the Ethics code, personal, non-business use of either the Internet or email must be limited to areas where there is no additional, easily quantifiable cost to the City. Users are not authorized to make personal use of any Internet sites that result in additional charge to City. It is the user's responsibility to be aware whether additional cost is involved. If a charge is incurred, the user must reimburse the City for such.

xii. Access to the City's all-inclusive ("everyone") email groups is restricted to Department Heads, senior leadership and to MHIS staff who may need to communicate with all users as part of the maintenance and operation of the City's information technology systems.

xiii. A user interested in notifying colleagues of a charitable purpose via email or any other City system must make a formal request to his/her Department Head or the Chief Information Officer before issuing any such communication. These requests will be considered individually and a determination made on a case by case basis.

xiv. Internet access and email, like all other forms of communication, reflect upon the City and users should maintain a professional and courteous tone, observing the rules governing conduct of employees.

xv. Email created or received by an employee of a government unit may constitute a public record and therefore may be subject to public access through the Freedom of Information Act (FOIA). The Connecticut State Library is charged by the State with setting policy for retention of documents. A determination as to whether an email message is exempt from disclosure depends upon the content of the message. Additionally, email messages may be discoverable in litigation and may be admissible in court or administrative proceedings. Like all electronically created and stored records, email is subject to the rules of evidence and a judge will rule on its admissibility.

i. In compliance with the direction of the State Librarian and applicable state and federal regulations, the City archives all email messages indefinitely.

ii. Pursuant to federal rules of practice, when the City reasonably anticipates litigation, any and all emails and electronically-stored information pertaining to the possible litigation must be preserved and stored. When in doubt, consult with Corporation Counsel regarding the need to preserve electronic records.

xvi. Under no circumstances is it permissible for employees, contractors, students, interns, volunteers, guests or other authorized users to acquire access to confidential data unless such access is required by their official duties. Under no circumstances may users disseminate any confidential information unless such dissemination is required by their official duties or authorized by law.

i. The City recognizes that employees may, from time to time, bring work home with them. Users are cautioned to be aware of the nature of any information they transport out of the office, either on laptops or removable media (such as CD-ROMs, "thumb drives" or "pen drives"). Confidential or otherwise legally protected information should be secured using some form of encryption to prevent accidental disclosure in the event of loss or theft of a laptop or external media.

ii. Examples of acceptable encryption techniques include password protected ZIP files, or thumb drives with built-in encryption. Password protection in Word documents, Excel spreadsheets and PDFs is readily broken and therefore is not acceptable protection. Users must immediately report any loss or exposure of confidential or protected information to their Department Head and the Chief Information Officer.

xvii. Any user with access to Criminal Justice Information (CJI) shall comply with the FBI Criminal Justice Information Services (CJIS) Security Policy. The security policy is developed per Title 28, Code of Federal Regulations (CFR) and the Federal Information Security Management Act of 2002.

xviii. Users must take care to avoid compromising the security of the network. All passwords should be kept confidential. Users who will be leaving their computers unattended should log off or lock their workstation. No user is allowed to access the Internet or other external

networks via a modem unless they have received specific permission from the Chief Information Officer.

xix. All messages created, sent or retrieved over the Internet are the property of the City, and should be considered public information.

   i. The City reserves the right to use any software to access and to monitor all messages and files on its computer systems as deemed necessary and appropriate including, but not limited to, site blocking software.

   ii. Internet messages are public communication and are not private.

   iii. Employees have no reasonable expectation of privacy in email communications or Internet usage occurring on City computers or in the workplace.

   iv. All communications including text and images can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

xx. Upon the transfer to another department, lay off, suspension, leave of absence lasting more than one (1) week or termination (voluntary or involuntary) of an employee/user with any computer or Internet access on the City's computer network, the Department Head and Human Resources Director shall notify the Chief Information Officer.

xxi. Department Heads shall request, in writing, for individual employees to have access to a computer, the Internet and E-mail through the City's system, certifying that said employee has business needs for such access.

xxii. Violation of this policy may result in limiting or revoking use of the City's information technology resources and/or disciplinary action up to and including termination. If necessary the City will advise appropriate law enforcement agencies of any illegal acts.

   i. The City reserves the right to change this policy at any time, with such notice, if any, as may be reasonable under the circumstances.

   ii. Employees may contact the Human Resources Department or MHIS for any questions they may have regarding this policy.