



# CITY of BATH, MAINE

## CITY OF BATH TECHNOLOGY USE POLICY

NOTE: The City of Bath's information and technology (I.T.) related communication equipment and resources may include, but are not limited to computer workstations, laptops, mobile devices, voice mail, networks, printers, copiers, telephones, modems, email, Internet and Intranet.

PURPOSE: The purpose of this policy is to set the minimum rules to be followed while using any or all of the City of Bath's I.T. equipment and resources.

BACKGROUND: The City of Bath, hereinafter referred to as the "City", provides its employees access to I.T. equipment and resources. Computers and the infrastructure that interconnects them are integral to the conduct of government functions. These resources are required to be used in an appropriate manner. This policy is intended to inform and advise City employees as to the appropriate use of these resources.

PRIVACY: Because all information and systems are the property of the City, personnel should not expect that messages are private. Information on the system has been classified as a public record and may be subject to disclosure under the Right to Know Law. Privacy is not guaranteed and should not be expected. E-mail received or created (incoming or outgoing) in the course of business is an official public record. Depending on the topic it may or may not be a *confidential* record under the Freedom of Access Act (FOAA).

MAINE FREEDOM OF ACCESS ACT: The State of Maine "Freedom of Access Act" (1 M.R.S.A., §401-410) clearly provides that any and all written, printed or graphic matter or any mechanical or electronic data compilation (files, notes, records, copies, etc.), regardless of the media used to store or transmit them (paper, film, microfiche, recordable media, electronic media, etc.) in public offices received or prepared for use in connection with the transaction of public governmental business is public property. As such, the public may have access to those materials for examination. The law places some very narrow restrictions on the public access, such as personnel files, certain investigation files, etc. but most materials are subject to public viewing. Employees are advised that there should be no expectation of privacy when using any City owned I.T. or related communications equipment or resources.

MONITORING: The City's computer infrastructure is provided for the purpose of conducting City related business and for City purposes. The City has a proprietary interest in its computer infrastructure and all information on its computer and as noted, the employees have no right or expectation of privacy with regard to use of the City's system. In using the City's computers, all employees consent to the monitoring of all communications and information transmitted, received or stored on the City's computers. The City Manager and his/her designee have the specific right to monitor all computer activities by employees of the City of Bath. In addition, employees should be aware that deleted files may be retrieved and read by the Department Heads or other Supervisory Personnel. The City reserves the right to retrieve, monitor

or review any messages in the City's network and may disclose such messages for any purpose without permission of the employee.

USE: The City's I.T. equipment is the property solely of the City of Bath and intended for the transaction of City business. City-owned I.T. equipment and resources are made available to employees to conduct official City of Bath business. Use of I.T. resources, such as e-mail, Internet, social networking media interfaces such as YouTube, Facebook and blogs, etc., are intended to be used for City business purposes. The City's employees are provided with a cityofbath.com email account through which to conduct city business. All city employees using city-owned I.T. equipment and resources are expected to comply with the following work rules:

1. Unless required to do so in the performance of official duties (e.g., law enforcement), City employees shall not use City-owned, City-leased, or City-controlled I.T. equipment or other resources to create, record, store, copy, transmit, distribute, image, modify, print, download, or display inappropriate or unprofessional materials that demean, denigrate, or harass individuals or groups of individuals, on the basis of any protected class including race, ethnic heritage, religious beliefs, disability, sexual orientation or gender regardless of whether the material was intended to demean, denigrate or harass any employee or group of employees. This prohibition applies to the use of City-owned equipment regardless of whether the employee is on-duty or off-duty. Intentional and substantial violations of this work rule are unacceptable and will not be tolerated. Intentional and substantial violations of this rule shall constitute just cause for termination.

2. Unless required to do so in the performance of official duties (e.g., law enforcement), City employees shall not use City-owned, City-leased, or City-controlled I.T. equipment or other resources to create, record, store, copy, transmit, distribute, image, modify, print, download, or display materials that are sexually explicit or pornographic in nature. This prohibition applies to the use of City-owned, City-leased, or City-controlled equipment regardless of whether the employee is on-duty or off-duty. Intentional violations of this work rule – regardless of whether they are of an incidental nature – are unacceptable and will not be tolerated. Any intentional violation of this rule SHALL constitute just cause for termination.

3. City employees shall not conduct City business through personal email accounts (e.g., Yahoo, Hotmail, and G-mail)

4. City employees shall not use City's technology resources to forward or otherwise broadcast mass communications that are not work-related, or solicitations for causes unrelated to the City's business, no matter how worthy the cause may be perceived to be. If in doubt as to whether your proposed e-mail meets these guidelines, contact your Human Resources office. Solicitations or mass communications for causes believed to be related to City business should be brief, not endorse any product or provider, and should refer readers to a webpage for further information. The City Manager or his/her designee must approve such solicitations or mass mailings.

5. City employees shall not use City-owned, leased, or controlled I.T. resources to conduct outside business nor shall they use these resources in conjunction with any outside employment activity.

6. State law makes it a crime to use a computer system operated by a City department or agency to advocate for or against a candidate for federal office, a constitutional office, an elective municipal, county or City office, including leadership positions in the Senate and House of Representatives, as well as to solicit contributions required by law to be reported to the Commission on Governmental Ethics and Election Practice.

7. With the specific exception of accessing pornography as described in Paragraph 2 above, any personal use of City-owned I.T. equipment and resources must be incidental in nature. Examples of incidental use may include but are not limited to, brief e-mails, accessing an appropriate subject on the Internet, phone calls of an urgent nature, using computer capabilities for incidental correspondence, etc. The use of City-owned resources represents a cost to the City and, as such, printing and copying for personal use is restricted to incidental use only.

INTERNET ACCESS. The City believes that the use of Internet resources facilitates communication, innovation, resources sharing, and access to information. Due to the complex nature of accessible networks and the magnitude of potential information available to employees using the Internet, it is mandatory that the use of the Internet by City employees be in an appropriate manner. It is to be remembered that access to and use of the Internet is a privilege and not a right.

Internet access provides the City with significant access and the opportunity to disseminate information to individuals outside the City. Since access to Internet messages are capable of being forwarded without the express permission of the original author, users must exercise caution in the transmission and dissemination of messages outside of the City and all such messages must comply with this Policy, other applicable City Policies and Ordinances, and all State and Federal Laws.

The City may also set up on-line forms on the Internet that will be used in place of paper communications. In each instance of use of these forms, a confirmation must be either sent via e-mail or regular written communication. These on-line forms will be handled in the same way and with the same amount of accountability as their written counterparts. It is the Department Head's responsibility to ensure that the electronic forms are processed appropriately.

ELECTRONIC MAIL (E-MAIL): Electronic mail, Internet mail, internal electronic mail and telecommunication access are resources available to City employees to communicate with each other, other government entities, companies and individuals for the benefit of the City. The City of Bath's electronic mail system, "e-mail", is designated to facilitate City business communications among employees and other business associates. Since no computer system is completely secure, and there is no expectation or right of privacy regarding use of the system or the information on the system, e-mail should not transmit sensitive material such as personnel

decisions or any other similar information where unauthorized access may be an issue.. Such information should be more appropriately communicated by written memorandum or personal contact.

E-mail messages reflect the City's image. The e-mail messages should be composed in a professional manner that is similar to messages sent on City stationary. Employees should keep in mind that electronic files may be subject to public disclosure under the Right to Know Law or may be otherwise accessible to the general public. It is expected that employees' statements and electronic messages in files will reflect favorably on the City and its employees.

Access to Public E-Mail Forms. Departments may, with the approval of the City Manager, set up "public" forms for residents and the public to send inquiries, comments, complaints or suggestions. The information on these forms will be forwarded to a designated individual or to the head of the Department concerned with the subject matter of the e-mail for processing. Due to the nature of e-mail, no response to an inquiry is guaranteed.

Confidential Passwords. Individuals may be assigned confidential passwords. Users should be aware that such an assignment does not imply that the system is for personal confidential communication. The use of the e-mail system remains for the conduct of City business. Passwords should be periodically changed to ensure the security of the e-mail system. Users should not share their passwords with anyone else.

Retention of E-Mail. E-mail messages are similar to printed communication and should be written with the same care. Employees should be aware that when they have deleted messages from their workstation mailbox, it might not have been deleted from the central e-mail system. The message may be residing in the recipient's mailbox or forwarded to other recipients. Furthermore, the message may be stored on the computer's back-up system for an indefinite period of time. (Please note that e-mail has been classified as a "public" document, i.e. available to the media, in at least one state. Keep that in mind when you create e-mail.)

Employees should delete e-mail messages as soon as possible after reading. An accumulation of files will degrade network performance and response times.

PROHIBITIONS. Each employee is responsible for his/her actions and activities involving use of the City's computer infrastructure. This document does not attempt, nor can it, state all of the required or prescribed behaviors that might arise in use of the City's system. The following prohibitions are specific examples of types of uses that are prohibited but are intended only as an illustrative list. Examples of this prohibited conduct include, but are not limited to the following:

1. The installation or use of unauthorized software or the introduction of any virus into the City's network.
2. Intentionally damaging the system or data, intentionally deleting data created by other users or causing harm to the system through the introduction of programs designed to harm data or degrade system performance.

3. Vandalism to the system which shall include any malicious attempt to harm or destroy any equipment, materials or data. This includes, but is not limited to, the uploading or creation of computer viruses.
4. Making illegal copies of City provided software.
5. Accessing, transmitting, or posting any material or communication that may be interpreted as:
  - A. Damaging to another's reputation.
  - B. Construed by others as disruptive, offensive, abusive or threatening.
  - C. Obscene or containing any sexually explicit images or messages.
  - D. Containing ethnic slurs, racial epithets or anything that may be construed as harassment or disparagement of others based on race, national origin, sex, age, disability, or religious beliefs.
  - E. Contrary to the City's Policy on Harassment.
6. Any illegal use including violations of any Federal or State Laws regarding computer use; unauthorized use of copyrighted material or contract related material without the owners' permission, except when the copying is a "fair use" under the copyright laws.
7. Solicitation or use for commercial ventures, religious or political causes, outside organizations, or other not job-related solicitations, unauthorized use for private, financial or commercial gain or for private or commercial advertising.
8. Use that wastes resources.
9. Gaining unauthorized access to computer resources, information, or entities.
10. Unauthorized use of another's account or password.
11. Posting material created by others without their consent.
12. Posting anonymous messages.
13. Intentional and unauthorized interception, eavesdropping, recording, reading, deleting, copying, altering, forging the electronic mail of others and deliberately interfering with the ability of others users to send/receive electronic mail; sending or forwarding frivolous e-mail containing attachments, images, and/or executable files.
14. Any other uses that may compromise the integrity of the City and its business in any way.

**ACTIONS:** The City Manager shall determine in all instances whether or not there has been violation of this Policy or of any other applicable City Rule, Regulation or Ordinance or any Federal or State Law or Regulation. Upon such determination, the Manager shall have available to him all of the following remedies:

1. Reimbursement. To require all City employees to reimburse the City for any losses, costs, telephone charges, or damages incurred by the City relating to or arising out of that employee's violation.
2. Revocation of Privilege. To revoke, limit or otherwise circumscribe the employee's use of and access to the City's computer infrastructure.

3. Discipline. To impose discipline in accordance with the City of Bath Personnel Policies and/or other applicable Rules, Regulations or Laws, up to and including dismissal.
4. Prosecution. Where the nature of the violation warrants, to refer the violation to the appropriate authorities for criminal prosecution.

EMPLOYEE TERMINATION, LEAVE OF ABSENCE, VACATION, ETC: Employees who leave employment with the City have no right to the contents of their e-mail messages and are not allowed access to the e-mail system. Supervisors or Department Heads may access an employee's e-mail if employees are on leave of absence, vacation, or are transferred from one Department to another Department and it is necessary for the City's business purpose.

REPORT OF VIOLATIONS. Each employee who observes a violation of this Policy or circumstances where the use of the City's computer resources is detrimental to the City or inhibits the City's ability to do its business, shall notify his/her immediate Supervisor, the City Manager, or the System's Administrator.

EMPLOYEE AGREEMENT AND VERIFICATION. An employee's use of the City's computer system constitutes that employee's agreement to abide by the City's Policy governing use of the system as set forth herein or as may be from time to time modified. All employees authorized to use or access the City's computer system shall be required to read and signify acceptance of their obligations under this Policy by signing an Agreement that acknowledges receipt, review and understanding of the Policy and an intention to follow and abide by the Policy.

AMENDMENTS. The City may amend this Policy from time to time as it deems to be in its best interests. Amendments shall be circulated to affected employees and shall be acknowledged and verified in the manner described above.