

The Metropolitan Government of Nashville and Davidson County

Internet and Electronic Mail Use Policy

I. Purpose

The Metropolitan Government provides Internet connections and electronic mail ("e-mail") for use by its employees in the performance of their duties.

The purpose of this Policy is:

1. To establish guidelines and minimum requirements governing the acceptable use of Metropolitan Government-provided Internet and e-mail services.
2. To educate employees regarding these guidelines and requirements.
3. To define enforcement mechanisms to ensure successful implementation of these guidelines and requirements.

II. Scope

This policy applies to all Metropolitan Government employees ("users"), including permanent, temporary and part-time employees, as well as interns and contractor personnel, whose access to, or use of, Internet and e-mail services is funded by the Metropolitan Government or is available through equipment owned or leased by the Metropolitan Government.

This policy is intended to illustrate the range of acceptable and unacceptable uses of the Metropolitan Government's Internet and e-mail facilities and is not necessarily exhaustive. Questions about specific activities not enumerated in this policy should be directed to the user's supervisor.

III. Objectives

This Policy is intended to achieve the following objectives:

- Facilitate Internet and e-mail usage for the benefit of the Metropolitan Government.
- Avoid disruptions to the Metropolitan Government's activities from unacceptable use of the Internet and e-mail services.
- Minimize the risks and unnecessary costs from Internet and e-mail usage.
- Increase productivity.
- Educate employees that Internet and e-mail communications are subject to the same laws, rules and regulations as offline office communications.
- Comply with the Metropolitan Code of Laws as well as State and Federal laws.
- Define personal responsibilities regarding acceptable and unacceptable usage of the Internet and e-mail, including but not limited to:
 - Confidentiality
 - Harassment

- Privacy
- Pornography
- Vandalism
- Network security
- Copyright infringement
- Unauthorized not-for-profit activities
- Personal for-profit activities
- Private activities
- Political campaign activities
- To comply with T.C.A. § 10-7-512's requirement that the Metropolitan Government adopt a written policy on monitoring of electronic mail communication.

IV. Background

The Internet and e-mail are useful tools for conducting the Metropolitan Government's internal business and activities with business partners and communicating with the public.

E-mail and Internet-generated electronic records that are created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions may be public records subject to public inspection. These records are subject to records management requirements under Metropolitan Code of Laws § 2.140.

In the course of their work, system administrators or other authorized individuals may monitor any user's Internet and e-mail activities at any time without the user's permission or notification. Additionally, the content of these activities may be monitored during investigations of inappropriate use or non-compliance with this Policy.

As with any Metropolitan Government-provided resource, the use of the Internet and e-mail should be limited to legitimate Metropolitan Government business and is governed by rules of conduct similar to those applicable to the use of other resources, including other information technology resources.

A. Internet-specific background

The Internet is a network of computer networks connecting educational institutions, government agencies and various commercial and non-profit organizations. Once an exclusive domain of research and education groups, the Internet is now a shared information resource for individuals, businesses and governments.

The Internet can help the Metropolitan Government by facilitating communication and collaboration, disseminating information and permitting the sharing of resources. The Internet can also be used to publish information required by law or executive order as well as information of general interest to the public.

Users of the Internet should be aware of certain characteristics that distinguish the Internet from other means of communication, such as paper records, telephones, and information stored on electronic media such as diskettes.

- Downloading and storage. Information downloaded or stored by users of the Metropolitan Government's Internet system can be accessed by the Metropolitan Government even if password-protected or encrypted. Use of passwords or encryption does not confer any special status on Internet-generated files.
- Internet browsing and establishing links are not private activities. The Metropolitan Government may employ screen-capture software or other technological means to monitor and record user's Internet activities.
- The Metropolitan Government may block access to sites that are inappropriate for use on the Metropolitan Government's equipment, such as sites that contain sexually harassing material.
- Content downloaded from the Internet occupies storage space and may interfere with storage of other material and disrupt operations on other parts of the Metropolitan Government's computer system. Although deletion of unnecessary content downloaded from the Internet is encouraged, users should consult the Metropolitan Government's record retention guidelines for proper instruction regarding disposal or archival of Internet downloads.

Cookies. Cookies are small files that are downloaded to a computer when during browsing of certain web pages. Cookies hold information that can be retrieved by other web pages on the site. Some cookies are programmed with an expiration date so that they are automatically deleted after a period of time. Cookies may be turned off and deleted.

B. E-Mail-specific background

E-mail refers to the electronic transfer of information, typically in the form of electronic messages, memoranda, and attached documents from a sending party to one or more receiving parties, via an intermediate telecommunications system.

E-mail can help the Metropolitan Government improve the way it conducts business by providing a quick and cost-effective means to create, transmit, and respond to messages and documents electronically. Well-designed and properly managed e-mail systems expedite business communications, reduce paperwork and automate routine office tasks, thereby increasing productivity and reducing costs.

As with the Internet, users of e-mail should be aware of certain characteristics that distinguish e-mail from other means of communication such as physical letters.

- The systems involved in the transmission and storage of e-mail messages may be "backed up" by systems administration on a routine basis. This process results in copying data, such as the content of an e-mail message, onto storage media that may be retained for periods of time and in locations unknown to the sender or recipient of a message.
- A user's e-mail account password or encrypting code does not confer a special status on e-mail records with respect to the applicability of laws, policies, and practices.
- All information transmitted via or stored on the Metropolitan Government's e-mail system can be reviewed by the Metropolitan Government.

- Inadvertent disclosure may occur when e-mail messages are forwarded to unauthorized users, directed to the wrong recipient or printed in a common area where others can read them.
- Transmission of e-mail to locations outside of the Metropolitan Government's local area network may require the use of the Internet. Since the Internet and its tools adhere to open and documented standards and specifications, it is inherently an unsecured network that has no built-in security controls.
- E-mail communications, if allowed to accumulate on a server, can quickly consume the server's disk space and may cause system problems. Although deletion of unnecessary e-mail communications is encouraged, users should consult their supervisor for proper instruction regarding disposal or archival of e-mail correspondence.

V. Potential Risks

Although Internet and e-mail access offer significant business benefits, use of the Internet and e-mail exposes Metropolitan Government users to various risks. Even with the extensive effort that has been made by the Metropolitan Government to minimize those risks, there is no known way to ensure complete protection. The most significant potential problems associated with the Internet and e-mail use are:

- Exposure of the Metropolitan Government to legal liability due to harassment, vandalism, intellectual property rights violations and other unauthorized internet and e-mail activities.
- Exposure of the Metropolitan Government to production of potentially damaging documents on record in the event of litigation.
- Exposure of the Metropolitan Government's network to computer viruses from the downloading and use of programs or files from Internet and e-mail sources. E-mail is the most frequently used method for transmitting computer viruses.
- Exposure of the Metropolitan Government network to outside unauthorized surveillance, forgery, downloading or vandalism.
- Exposure of confidential Metropolitan Government records (including passwords, sensitive data or correspondence) to breaches of data security from unauthorized intrusion.
- Productivity problems resulting from spending significant amounts of time using the Internet's vast social and informational forums for activities unrelated to Metropolitan Government business.
- Productivity and other problems resulting from use of the Internet and e-mail for unauthorized non-profit or private for-profit activities.
- Productivity and other problems resulting from use of the Internet and e-mail for political campaign activities.
- Consumption of limited disk storage on the Metropolitan Government's servers and on user PCs with unnecessary information that has been downloaded from the Internet or received via e-mail.

Thus, each authorized user must exercise prudence and caution in using these powerful information resources. The sections that follow define responsibilities for ensuring that Internet services and e-mail are used appropriately.

VI. Principles of Acceptable Use and User Responsibilities

This Policy is intended to illustrate the range of acceptable and unacceptable uses of the Metropolitan Government's Internet and e-mail facilities and is not exhaustive. Supervisors or department heads may authorize the use of the Internet or e-mail relating to the official functions of the Metropolitan Government. All authorized employees are encouraged to use the Internet and e-mail as they would any other communication tool provided by the Metropolitan Government subject to the following conditions.

The use of the Internet and e-mail services should be dedicated to legitimate Metropolitan Government business and is governed by internal policies as well as local, State and Federal laws. Acceptable use must be responsible, legal and ethical. Users should demonstrate cost-effective consumption of shared resources and respect for intellectual property, ownership of information, system security mechanisms and individual rights to privacy and freedom from intimidation, harassment and annoyance.

Each user has the following responsibilities:

- Each user will certify that he or she has read and fully understands the contents of this Policy by signing the attached agreement.
- Each user must comply with this "Internet and Electronic Mail Use Policy."
- Users must be aware of the classification of any information contained in data files or correspondence which they are transporting using the Internet and e-mail.
- Under no circumstances should data ever be transported that would place the Metropolitan Government in violation of any law.
- The content of anything exchanged (sent or received) via Internet or e-mail (regardless of its state of encryption) must be appropriate and consistent with the Metropolitan Government's Policy, subject to the same restrictions as any other exchange.
- Users should use appropriate precautions when confidential information is contained in e-mail communications. These precautions should protect confidential and sensitive information where intentional, inappropriate, or accidental disclosure of the information might expose the Metropolitan Government or an individual to loss or harm.
- Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of their e-mail account by unauthorized individuals.
- Users must use Internet and e-mail in a manner that is consistent with their job function, even when the access is off-hours.
- Each user must be courteous and follow accepted standards of etiquette.
- Each user must respect system security mechanisms.

VII. Acceptable Usage

Acceptable Internet and e-mail activities are those that conform to the purpose, goals and mission of the Metropolitan Government and to each user's job responsibilities. The following list, although not all-inclusive, provides some examples of acceptable usage:

- Communications, including information exchange and storage, directly relating to the mission, Charter and work tasks of the Metropolitan Government.
- Communications, including information exchange and storage, for professional development or to maintain job knowledge or skills.
- Use in applying for or administering grants or contracts for the Metropolitan Government.
- Research for the benefit of the Metropolitan Government.
- Communications with the Metropolitan Government's business partners providing document delivery or transferring working documents or drafts for comment.
- Use for advisory standards, research, analysis, and professional society or development activities related to the user's responsibilities for the Metropolitan Government.
- Announcements of the Metropolitan Government procedures, policies, services, meetings, or activities.
- Incidental personal use of the Internet and e-mail to exchange or store personal information. This information will not be treated any differently than other information on the Metropolitan Government network system.

VIII. Unacceptable Usage

Unacceptable uses are those activities that do not conform either to the purpose, goals, and mission of the Metropolitan Government or to a user's job responsibilities. Any Internet and e-mail usage in which acceptable use is questionable should be avoided. When in doubt, seek Policy clarification from your supervisor prior to pursuing the activity. The following list, although not all-inclusive, provides some examples of unacceptable usage:

- Private or personal for-profit activities. This includes use of Internet and e-mail services for private purposes, such as marketing or business transactions, private advertising of products or services, and any activity meant to foster personal gain.
- Unauthorized not-for-profit business activities. This includes the conduct of any non-Metropolitan Government-related fund raising or public relations activities such as solicitation for religious and political causes.
- Use for, or in support of, prohibited activities as defined by Federal, State and local laws or regulations. Illegal activities relating to Internet and e-mail access include, but are not limited to:
 - Transmission of threatening, offensive or harassing information (messages or images) which contains defamatory, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.
 - Violating Federal and State laws dealing with copyrighted materials (including articles and software) or materials protected by a trade secret. Users may access copyrighted material, but its use must be strictly within the agreement as posted by the author or current copyright law. The Federal Copyright Act at 17 U.S.C. 101 et. seq. (1988), protects and prohibits misuse of all original works of authorship in any tangible medium of expression. This includes a prohibition on plagiarism.
 - Transmission of incendiary statements that might incite violence or describe or promote the use of weapons or devices associated with terrorist activities.

- Intentionally seeking information about, obtaining copies of, or modifying contents of files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users.
- Violating the privacy of individual users by reading their e-mail communications unless specifically authorized to do so.
- Attempting to subvert network security, to impair functionality of the network, or to bypass restrictions set by the network administrators. Assisting others in violating these rules by sharing information or passwords is also unacceptable behavior.
- Deliberately interfering or disrupting another user's work or system. Users must not perform any activity that will cause the loss or corruption of data, the abnormal use of computing resources (degradation of network performance), or the introduction of computer worms or viruses by any means.
- Distributing "junk" mail or "spam", such as chain letters, advertisements, or unauthorized solicitations.
- Distributing the Metropolitan Government's data and information without authorization.

IX. Enforcement

Each department head or director is responsible for implementation and enforcement of this Policy, including but not limited to monitoring of Internet and e-mail use and application of appropriate corrective actions. The Information Systems Department retains e-mail communications for the sole purpose of backup for a specified period of time. The archiving and retention of public records contained in e-mail communications is the responsibility of the individual departments and must be in accordance with State law and policy adopted by the Public Records Commission.

A. Monitoring

- System administrators will not routinely monitor user Internet and e-mail activities, and will take reasonable precautions to protect user privacy. Testing performed by internal audit or the authorized Metropolitan Government personnel as necessary. Users should be on notice that the maintenance and operations of the Metropolitan Government network may result in observation of random user activities. The Metropolitan Government may monitor user Internet and e-mail activity, however, for reasons including but not limited to:
 - Legitimate business purpose (e.g., the need to access information when a user is absent for an extended period of time or unavailable).
 - Diagnosing and resolving technical problems involving system hardware, software, or communications.
 - Conducting network maintenance.
 - Investigating possible misuse of Internet and e-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.
 - Gathering necessary information in the event of litigation.
 - Investigating a possible crime or violation of this Policy.
 - Disclosing any e-mail or Internet activity to law enforcement officials whenever legally required to do so.

X. Corrective Actions

The Metropolitan Government will review alleged violations of this Policy on a case-by-case basis. Clear and willful violations or abuse of acceptable usage will lead to appropriate disciplinary actions, depending upon the severity of the transgression and Policy abuse, up to and including termination. Criminal or civil action may be initiated in appropriate instances.

A user's access to Internet and e-mail may be suspended, with or without notice, when deemed necessary for the operation or integrity of the Metropolitan Government's communications infrastructure, connected networks or data.

XI. Written Agreement Required

Users having access to Metropolitan Government-provided Internet or e-mail services are advised that all such network activity is the property of the Metropolitan Government. All users of Internet and e-mail services are required to acknowledge acceptance of, and intention to comply with, "Internet and Electronic Mail Use Policy" by signing an "Internet and Electronic Mail Use Agreement." The attached "Sample Internet and Electronic Mail Use Agreement" is provided as a model. Signed agreements will be maintained by each department.

XII. Waiver of Privilege Not Intended

Nothing contained within this policy is intended to waive any privileges provided by law.

The Metropolitan Government of Nashville and Davidson County Internet and Electronic Mail Use Agreement

I hereby agree that I have read the attached document entitled "The Metropolitan Government of Nashville and Davidson County Internet and Electronic Mail Use Agreement," and certify that I am familiar with the contents of the document and agree to comply with its terms.

I also acknowledge my understanding that any infractions on my part may result in disciplinary action including, but not limited to, removal of e-mail services, removal of Internet services, suspension of access to computers and networks, suspension of employment, termination of employment, and recommendation for prosecution.

User Name (Print): _____

User Signature: _____

Date: _____

The Metropolitan Government of Nashville and Davidson County Internet and Electronic Mail Use Policy