City of Annapolis

Electronic Use Policy

1.0 PURPOSE:

Compliance with this administrative regulation will encourage responsible and acceptable use of **electronic communications** provided by the City of Annapolis [City], and will support the needs of citizens and City employees. This administrative regulation reflects a realization that efficient use of electronic communications can:

- Enhance partnership, community involvement and the exchange of information and ideas between citizens, businesses and local government.
- Provide information both internally and to the public about the activities and services of the City.
- Improve the quality, productivity and general cost-effectiveness of the City's work force.

2.0 ORGANIZATIONS AFFECTED:

All departments/divisions. This administrative regulation applies to all **users**.

3.0 DEFINITIONS:

3.1 Electronic Communications - includes all forms of electronic communications systems, components and data. Examples include but are not limited to, the City's web site, intranet, Internet service, software, e-mail, network infrastructure, telephone service, long distance service, cell phones, pagers, fax machines, copiers, video services, imaging, wired and Awireless @ network communications.

3.2 MIT Committee -Management Information Technology Committee

3.3 MIT Liaisons - individuals appointed by their department director who represent their department in the MIT Committee on IT related issues.

3.4 Cell Phone - for the purposes of this policy, any mobile, wireless device providing transmission of voice, data, or video excluding devices attached to the City's radio system. This would include such wireless mobile devices as Cell phones, PDAs, etc.

3.5 Users - employees, contractors and vendors who use City-provided electronic communication systems, components and data, including but not limited to computers, cell phones, desk phones, fax machines, personal digital assistants (PDAs), pagers, copiers, connectivity to the City network, Internet, intranet, computer hardware, software and e-mail.

3.6 Unauthorized Equipment or Software - equipment or software that has not been approved by MIT or is not properly licensed to the City.

3.7 Network infrastructure - all equipment and services that support the transmission of voice, video and data. This includes all access points to the network, connectivity between sites, connectivity within sites, security of the network, and security of all associated data.

3.8 MIT - Management Information Technology Department.

3.9 Guidelines for Electronic Communications - A set of informational guidelines available on the City Intranet which gives the current recommendations on usage and availability of electronic communications.

4.0 POLICY:

4.1 Departmental Responsibilities:

4.1.1 Initiating Requests for Electronic Communications:

Departments and any other entities authorized to use the City's electronic communications resources are responsible for initiating requests for access. Department Directors will designate a representative authorized to initiate requests for each type of electronic communication. This representative may or may not be the same individual as the MIT Committee Liaison.

4.1.2 Communication to Employees and Adherence to this policy:

The department of Human Resources [HR] is responsible for maintaining signed copies of this policy for each employee. Policies signed by employees should be put in their respective personnel file. Departments will ensure that all contractors and other persons being granted access to the City's network or other equipment comply with the terms of this administrative regulation. Policies signed by contractors or affiliates should be filed in their contractor or affiliate file.

4.1.3 Initiating Termination of Electronics Communications:

When a **user** with any form of City electronic communications leaves City employment or is no longer eligible for access, the designated departmental representative must notify MIT immediately. Disposal of user personal records such as e-mail and other messages will be disposed under the direction of the department director and according to City records retention policy.

4.1.4 Costs Incurred Due to Irresponsible or Improper Use of Electronic Communications:
Departmental personnel should be aware that the City's electronic communications components could be disrupted or compromised due to either malicious or unintentional acts or connections. Departments are responsible for any costs for damaged electronic communications components. This includes, but is not limited to the cutting of cables supplying connectivity to a departmental site and all other damages to any infrastructure.

4.1.5 Designation of MIT Committee Liaison:
Department Directors are responsible for appointing an MIT liaison.
MIT liaisons are responsible for:

Actively representing their departments at the scheduled MIT Committee meetings. It is important that the MIT Committee liaisons make the Committee aware of the needs of their departments.

Coordinating their departments with the Committee and the MIT Department in the City-wide IT initiatives including, but not limited to, such things as electronic communications, PC Lifecycle, enterprise licensing agreements, virus removal and updates, software license documentation, and other IT initiatives.

4.2 User Responsibilities:

Users of City-supplied electronic communications are responsible for showing reasonable effort in protecting the City's assets. This effort includes, but is not limited to, the following:

4.2.1 Initiating Requests for Electronic Communications Access:
Before a person is granted any form of electronic communication, the person must read and sign a copy of this administrative regulation stating that the person has read and understands its terms [accepted??]. Policy and guidelines for use of electronic communications are posted on the City's intranet.

4.2.2 Use of Electronic Communication Systems, Components, and Data:
All forms of electronic communication are resources granted to increase productivity and provide opportunities for professional growth. They must be used with these goals in mind.

Each user of a City-provided electronic communications resource is responsible and accountable at all times for the proper use of that resource. All users are expected to know the tools, rules and etiquette associated with each form of electronic communication as defined by the City, and to behave accordingly.

Users are responsible for knowing and abiding by the City's and department=s policy and guidelines for use of electronic communications.

Users must use all forms of electronic communications in accordance with all applicable laws and regulations. This includes compliance with copyright and license laws covering software, data and written material accessed, obtained or provided to others via the Internet.

Users shall secure all electronic communications components at all times. Users shall not allow unauthorized parties to use City electronic communications components.

Users shall protect passwords, access codes and other authentication devices. These are provided for security and shall not be shared with anyone. Electronic communication devices or components shall not be set to automatically retain passwords.

The City reserves the right to access, view and copy any user's electronic communications messages, files, data, correspondence, log files, etc. created by or stored on a City-owned electronic communication system or device. The City reserves the right to use the data and/or content for any purpose.

If any user has a question about the application of this Administrative Regulation, that user must seek clarification from his or her supervisor or MIT department.

4.2.3 Additions, Modifications or Changes to the City's Electronic Communications Systems and/or Components by Users:

Users shall not modify any electronic communication system, device, or component or its configuration. Examples include, but are not limited to disabling or removing virus protection or security software, and attaching or installing unauthorized equipment or software. Such actions could:

- be security risks
- jeopardize the stability of systems
- deny service to other City users
- present a licensing risk and legal liability to the City
- render the approved software inoperable
- nullify maintenance contracts

4.3.1 Management and Administration of Electronic Communication Systems, Components, and Data:

The Management Information Technology Department is charged and entrusted with the maintenance and security of electronic communications systems and components which includes, but is not limited to:

- monitoring the use of City electronic communications resources
- preserving the City's finite resources for their primary intended uses
- restricting access by users or groups
- blocking access to internet sites
- filtering email as deemed appropriate by MIT Committee and the Manager of MIT
- blocking of uploads and downloads of software and data

5.0 ACCEPTABLE USE:

The City's electronic communication systems have been installed in order for users to conduct City business. Use of the systems is for City business purposes as described in this document. Use of the systems for educational, training or other self-improvement purposes is authorized only if previously approved by the user's department head.

6.0 PROHIBITED USE:

Prohibited uses of any form of electronic communication include, but are not limited to, the following:

- Using the City's electronic communications for private gain or for profit, or to solicit for political, religious, non-City approved charities, commercial or other non-City business purposes.
- Violating the privacy of others. Users must respect the fact that Internet news group postings, certain e-mail messages, Web sites and various other communications on the Internet are public, and refrain from disclosing confidential and personal information.
- Using City electronic communications for non-business related activities including, but not limited to:

    - chain letters
    - greeting cards
    - personal usage of internet radio, TV or chat
    - outside e-mail services such as Hotmail, Yahoo and AOL
    - subscriptions to non-business related e-mail services
    - use of City telephone long-distance services for non-business-related purposes

- Using or storing files containing obscene, offensive, racial, sexual or hate language or images; engaging in ridicule; transmitting threatening, racial, sexual, obscene or harassing materials; or engaging in any form of sexual harassment.
- Interfering with or disrupting any City network or Internet users, services, programs or equipment. Disruptions include but are not limited to propagation of computer worms, viruses or other debilitating programs, and using the City network to make unauthorized entry into any other machine accessible via the network or Internet. Deliberate attempts to degrade or disrupt system performance may constitute criminal activity under applicable state and federal laws.
- Creating and/or maintaining personal files with obscene, offensive, racial, sexual, or hate language or images.
- Unauthorized sharing of secured or confidential data.

7.0 WARNINGS AND DISCLAIMERS

7.1 Privacy and Anonymity:

Users should have no expectation of privacy related to electronic communications usage. Most data and messages in hardcopy or electronic format is considered public record and is subject to the Freedom of Information Act. This includes, but is not limited to, such things as:

- E-mail content
- Telephone call records
- Internet activity records
- Files stored on City equipment

The City's Internet/e-mail host computers are traceable to the City. Persons using City-provided Internet/e-mail accounts should not assume they are given any degree of anonymity. The identification of electronic communication devices associated with the City can easily be accomplished.

7.2 Content and Confidentiality:

A wide variety of information exists on the Internet. Some persons may find part of that information to be offensive or otherwise objectionable. Users should be aware that the City has no control over, and therefore cannot be responsible for, the content of information on the Internet other than what we as an organization place there.
Users must understand that e-mail messages and other transfer of information via the Internet may not be secure. Persons desiring to send someone confidential or sensitive communications should consider the propriety of using the Internet/e-mail before using this tool in those situations.

8.0 ENFORCEMENT:

8.1 Investigations of Violations:

Departments will be responsible for the enforcement of the City's electronic communications policy. The Management Information Technology Department will assist in appropriate investigations, supplying usage detail and technical information where available, upon proper request. Department directors will take appropriate corrective action when their staffs do not adhere to this administrative regulation.

8.2 Disciplinary Procedure for Violations:

Violations of this administrative regulation may result in disciplinary action, including termination of employment.

9.0 PROCEDURES FOR SPECIFIC FORMS OF ELECTRONIC COMMUNICATIONS:

9.1 E-mail via GroupWise and/or Internet:

All users' e-mail and other Internet communications stored on City computers are the property of the City of Annapolis. Routine backup of electronic mail will occur as part of the system security policy procedure as defined and performed by MIT.

Electronic mail (both internal and via the Internet) stored on City computers may be subject to public disclosure.

Mass e-mailings require approval by a Department Head. Such broad-scale distribution slows down the system and impairs the efficient use of the Internet/e-mail systems by other people. For the same reasons, users shall avoid sending non-business e-mail.

Users shall not send unprotected, sensitive data over the Internet according the City Privacy Policy. This includes information such as Social Security numbers.

The City may review the Internet sites accessed by a user, and use that information for any purpose.

9.2 Network:

The MIT Department is responsible for protecting the City network. This includes all access points to the network, connectivity between sites, connectivity within sites, security of the network, and security of all associated data.

The attachment or installation of unauthorized equipment or software to the City's data or voice networks is prohibited. This could be a security risk, jeopardize the stability of the network and/or deny service to other City users.
The modification of the City's data or voice networks is prohibited. This could be a security risk and may jeopardize the stability of the network and/or deny service to other City users.

9.2.1 Remote Access to City Network

9.2.1.1 Dial-In Access to City Network - RESERVED

9.2.1.2 Virtual Private Network [VPN] Access to City Network -- RESERVED

9.3 Internet/Intranet:

9.3.1 Web Site

Department directors should appoint a person or team to coordinate the development and content of departmental pages. All pages are subject to format and content guidelines determined by the Website management team.

The Website management team has established web page design templates, content suggestions and posting procedures. Users wishing to create web pages should coordinate this work with the members the Website management team.

Departments are encouraged to include the www.annapolis.gov City web site addresses on business cards, brochures, newsletters, correspondence, advertising and other printed and promotional materials.

Departments may not create or contract for their own web sites, or acquire or use a domain name other than www.annapolis.gov, without prior approval of MIT.

Departments and other entities using space on the City's Web site are responsible for the development, content and accuracy of their pages. Information should be updated regularly.

9.4 Desk Phones:

9.4.1 Long Distance:

As with all forms of electronic communications, departments are responsible for granting access and ensuring that the usage is appropriate for their employees' job responsibilities.

9.4.2 Equipment:

All City-owned desk phone equipment is shall be purchased, distributed, inventoried and controlled by the Central Services department.

9.5 Wireless Devices:

A wireless device is defined as any mobile, wireless device (portable computers, cell phones, pagers, PDAs, PCSs, Nextel, etc.) providing transmission of voice, data, or video excluding devices attached to the City's radio system.

9.5.1 Cell Phones:

The purpose of a cellular phone is to improve employee efficiency, enable employees to respond promptly in emergency situations, and/or provide safety for the City of Annapolis citizens and employees when more conventional and cost effective means of communication are not available.

Information generated on, processed by, or stored in the City's cellular telephones, as well as all related billing records, may be provided to the public, including the press.

9.5.1.1 Eligibility:

Eligibility of employees for issuance or use of a City-owned cellular phone is governed by several factors:

Pagers are the preferred method for maintaining contact with mobile employees and should be considered prior to requesting a cellular phone. All cellular phones must be justified under at least one of the following categories and include an explanation of how the phone will be used in the conduct of City business and what the estimated frequency of need is:
Public/Personal Safety- the cellular phone user requires immediate direct communication with local police, fire and/or emergency medial units or agencies in order to provide for the safety of citizens or employees.
Accessibility- the cellular phone user requires immediate direct communication to conduct urgent City business and typically has no access to a conventional telephone, and/or it will be more cost effective than the employee seeking alternative methods of completing the task.
Responsiveness- the cellular phone user requires immediate direct communication to conduct urgent City business to ensure responsiveness to operational and/or support functions.

9.5.1.2 Departmental Responsibilities:

The Department Directors are require to ensure that justification and procurement regulations are followed, monthly bills are reviewed, and that reimbursement procedures for personal use are followed.
Cellular phone justification must address alternatives, and why a cellular telephone constitutes the most cost effective alternative for meeting operational requirements. As outlined on the Cellular Phone request Form, alternative forms of communications considered must include pagers and City/public telephone systems.

9.5.1.3 General Responsibilities:

Each cellular phone user is responsible for taking reasonable precautions to ensure that the cell phone is not lost or stolen. This includes making sure that the phone is contained in a secure storage area when not in use.

If a cellular phone is lost or stolen, the employee must report the loss to MIT by the next regular business day.

All City-owned cellular phone equipment and services will be purchased through (what department?).

9.5.1.3.1 Cell Phone Usage Responsibilities:
Cellular phone usage is governed by the following polices:
Use of a cellular phone should not be for convenience. Cellular phones should be used only when more conventional and cost effective means of communication are not available.
Cellular phones must be used responsibly, safely and in the interest and furtherance of the public's business.
Personal use of all City-owned cellular telephones (for both incoming and outgoing telephone calls) should be limited to infrequent, incidental and/or emergency purposes.
Length of cell phone calls should be kept to the minimum required to perform the job function. If calls of a longer duration need to be made, an alternate form of communication should be used, if possible. This does not apply in cases of emergency.
In order to better ensure the safety of our employees and citizens, City employees shall pull off the road to the nearest safe and practical location and stop their vehicle to take or complete any incoming cellular phone call. For outgoing calls, employees shall pull off the road to the nearest safe and practical location, stop their vehicles and then initiate any outgoing call.

9.5.1.3.2 Prohibited Uses of Cell Phones:
Any call which could suitably be made from a standard City telephone or by other electronic communication other than the City's trunked radio system.
Out-of-country calls, long distance calls and/or calls resulting in roaming fees, except in rare cases, and then only for business purposes.
Any call made in relation to an employee's private gain, profit or personal business enterprise including soliciting for political, religious, or other non-City business uses.
Any call for the purpose of entertainment, such as 900 numbers, movie links, etc.

9.5.1.3.3 Usage Reports:

9.6 Personal Computers and Peripherals -- RESERVED

9.7 Facsimiles -- RESERVED

9.8 Copy Machines -- RESERVED

9.9 Hardware -- RESERVED

9.10 Software -- RESERVED

9.11 Consulting Services -- RESERVED