Use of Electronic Systems & Tools Policy

Original/Revision Date: 06/15/1996; 03/01/2011; 09/22/2017

Purpose
The purpose of this policy is to set forth guidelines for the use of the City of North Miami Beach's (the City) computers, Internet, e-mail, and other electronic systems, which shall collectively be referred to as "computer systems." This policy is inclusive of all authorized users of the City's computer systems, which includes employees (permanent, temporary, seasonal, fulltime and part-time), interns, contractors, and others, including elected officials, who may be granted access by City management. Computers specifically identified and provided for use by the public in facilities such as the City Library, Resource Centers, the Computer Lab at the Y.E.S. Center, or other similar facilities are NOT included.

General Statement of Policy
The City computer systems shall be used to promote the City's mission, goals, and objectives, and shall be consistent with City policies. Specific rules and regulations relevant to the use of the City's computer systems may be implemented or modified as necessary to address technical, legal or management requirements.

Limited Purpose
The City computer systems may be used for research, business communications, and other uses relevant to City business.

Use of System is a Privilege
The use of the City computer systems is a privilege. Failure to comply with this policy could result in any one or more of the following: suspension or cancellation of access privileges, payment for damage and repairs, discipline, up to and including termination, or civil or criminal liability. The privilege to use the City computer systems may be administratively suspended or cancelled with or without notice at the sole discretion of City management.

Operations Parameters
The City cannot and does not guarantee that the City computer systems will be operational or available for use at all times. The City computer systems may be inoperable from time to time for brief or extended periods due to repairs, maintenance, or other factors. The City computer systems may also be intentionally restricted for security reasons. For these reasons Internet access and e-mail in particular may not be available, or may not be fully functional, or may not reliably retrieve or deliver messages. Users are advised not to rely exclusively on Internet access or e-mail for critical business transactions.

The City will take reasonable precautions to shield all of its computer users from potentially unwanted, intrusive, or offensive interruptions from external computer systems. Towards that goal, the City employs various technologies including web site blockers, white lists, black lists, SPAM filters, firewalls, anti-virus scanners,· and others. As newer technologies become available, they will be considered for implementation. However, the City cannot and does not guarantee that users will be completely protected at all times from unwanted, intrusive, or offensive computer materials.

Authorized Users
Anyone assigned a user ID and passwords from the City are the ONLY PERSONS AUTHORIZED to use City computers. The only exception to this rule involves authorized contractors hired by the City and given a user ID and password for limited network access.

Authorized individuals shall NOT give their passwords to any other person. If an authorized user must access another user's computer system, access will be provided by the Information Technologies Division (LT. Div.) or a person approved by the I.T. Division.

Unacceptable Uses
Unacceptable uses of the City computer systems, including e-mail and Internet access, include, but are not limited to, the following:

1. Deliberately accessing, reviewing, uploading, downloading, storing, printing, posting, transmitting, receiving or distributing pornographic, obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or sexually explicit material; material or information that use language or images that are inappropriate or disruptive to the business environment; materials that use language or images that advocate violence, or discrimination toward other people such as hate literature, or that may constitute illegal harassment or discrimination.
2. Knowingly or recklessly posting false or defamatory information about a person or organization, harassing another person, or engaging in personal attacks, including attacks based on unlawful discrimination.
3. Engaging in any illegal act or violating any local, state, or federal statute or law.
4. Vandalizing, damaging, or disabling the property of another person or organization; deliberately attempting to degrade or disrupt equipment, software, or system performance by spreading computer viruses or by any other means; tampering, modifying or changing the City's computer software, hardware, or wiring; and using the City's computers in such a way as to disrupt the use of the system by other users.
5. Gaining unauthorized access to information resources, the City's computers or any other system throughout the City; accessing another person's materials, information, or files without the direct permission of that person; logging in through another person's account; or using computer accounts, access codes, or network identification other than those assigned to the user without authorizations.
6. Violating copyright laws, or usage licensing agreements, or using another person's property without authorization, including the downloading or exchanging of pirated software or copying software to or from any City computer system.

If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the incident to their supervisor or the I.T. Div. so that this site can be added to a database of disallowed sites. This disclosure may also serve as a defense against an allegation that the user has intentionally violated this policy. A user may also, in certain rare instances, access otherwise unacceptable materials if necessary to complete a job function, and if so, shall be done with the prior approval of the City Management. In this circumstance, the I.T. Div. must be notified of this need in writing.

Expectation of Privacy
The City uses monitoring software and other technologies to assist users, to implement software fixes and upgrades, to ensure that City policies are followed, and to collect statistics. Information on every computer system user, including, but not limited to, user ID, date, time, IP address, where the user went or attempted to go on the Internet, e-mail messages sent and received, including content, and more are monitored and collected.

Furthermore, all information obtained using City computer systems, including e-mail messages sent or received and their content, may be considered public records under Chapter 119 of the Florida Statutes, commonly referred to as the "Public Records Law." All information contained on City computer systems, including any and all personal e-mail messages and their content and all files of any type, are subject to public disclosure. Additionally, all e-mail messages and their content and all files of any type contained on City computer systems, whether business or personal, are the property of the City of North Miami Beach and users have NO individual ownership or privacy rights regarding these items.

The City has the right to conduct an investigation of any individual user's City computer system activities and resources if there is a reasonable suspicion that the search will uncover a violation of law or City policy. Additionally, routine maintenance and monitoring activities may lead to a discovery that a user has violated this policy, another City policy, or the law. The City will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activity not in compliance with City policies.

City Software

Software is automatically protected by federal copyright law from the moment of its creation. Federal copyright law makes it illegal to copy a piece of software for any reason other than as a backup without the permission of the copyright holder.

For the City's purpose, illegal or unauthorized software is defined as any software that has not been approved by the City LT. Div. and/or any software for which the City has not purchased a license. Copying of illegal or unauthorized software to any system can result in contracting a virus, which can spread and cause serious damage to any or all systems. All City software contains a license identifier linked to the City of North Miami Beach and should not be used by any other person or entity.

1. Copying of City software is not allowed. Absolutely no software is to be copied from the network to a floppy disc or any other system without approval from the I.T. Div.
2. Copying of unauthorized software to the network or to any City computer is not allowed.
3. Any software that may be unique to your specific function within the City and that will only need to be installed on your system must still be approved by the I.T. Div.
4. Absolutely **no** illegal software is to be loaded onto any City computer. The I.T. Div. Manager must approve all software.
5. **New Software Purchases:** All software purchased for use on any City computer must be pre-approved by the LT. Div. for validity, compatibility and licensing. Software purchases will not be approved without the signature of the LT Div. Manager.
6. **Software spot-checking:** Designated LT. Div. personnel have the authority to audit, without notice, any City computer for unauthorized use and illegal software installations.
7. **Demonstration Software:** All demonstration software must be approved by the LT. Div. prior to loading onto any City computer.
8. **Personal Software:** Software that is not licensed and owned by the City of North Miami Beach is not permitted on any City computer. If the software is needed for the employee to be productive in his/her job, then the City should purchase a legal copy of the software for the employee's use.

Any illegal or unauthorized software installations will be removed immediately and will be reported, detailing the specific location of the incident, the type of software, and any "damages" that may have resulted from the illegal installation.

City Computer Hardware

1. New Hardware Purchases: The I.T. Div. must approve all new purchases of computer and/or related peripheral equipment. Hardware purchases will not be approved without the signature of the I.T. Manager.
2. Personal Use of City Computer/Peripherals: Personal use of City computers and/or related peripheral equipment is not permitted except for occasional, infrequent and incidental use which does not interfere with the normal job duties of the user or City operations. Excessive use which detracts in any way from job performance or City operations will subject the user to disciplinary action up to and including dismissal.
3. Moving Computer Equipment: Employees may not remove equipment from City property or employee's work area unless authorized by the LT. Div. and the City Manager. Moving of computer equipment within the City shall first be cleared through the LT. Div. When possible, LT. Div. personnel should supervise the move to insure proper installation and configuration of the equipment after it has been moved.
4. User to Maintain Equipment in Good Working Condition: Users should routinely clean computer equipment (dust, clean keyboard, mouse, and monitor) to maintain equipment in good working condition.
5. Policies to prevent Damage to Equipment:
    A. Beverage containers and food shall not be placed near computers, keyboards, mice, printers, or any other computer equipment.
    B. Eating and/or drinking over computer equipment shall not be permitted.
    C. Plants should not be located above or near any computer equipment.

D. Computer equipment is not to be installed below or adjacent to equipment or structures that are likely to leak or splash fluids, such as water fountains, room air conditioners, exposed water lines, drains, planters, open windows or known persistent leaks.

6. Personal Computer Equipment: Personal computer equipment shall not be connected to the City's network or any City owned computer/technology related equipment. Examples of such personal equipment include but are not limited to: printers, scanners, keyboards, mice, monitors, digital cameras, card readers, laptops, cell-phones, portable storage media such as thumb drives, etc. An exception is made only for vendors and contractors who are working on City equipment or working on behalf of the City, and have been approved by the I.T. Div.

Internet Use Agreement

1. Authorized users are responsible for properly using the Internet.
2. The Acceptable Use Policy shall be read and signed by the employee before computer system use including Internet access will be authorized.
3. Authorized users may not remove their name or domain information from postings or access anonymously to conceal their identity.
4. Authorized users may not lend out their e-mail accounts to other people.
5. Authorized users may not allow non-employees to access the Internet through City facilities without prior approval of the I.T. Div.
6. Spamming is the automated sending of messages to large numbers of newsgroups or people simultaneously. This is different from a legitimate e-mailing list because spamming is indiscriminate and unsolicited. Spamming is strictly prohibited.
7. Internet e-mail is provided to employees for business use. Users are advised not to indiscriminately provide their City e-mail address to non-business contacts, surveys or solicitations from mass-marketers.
8. If City users receive e-mail in their in-box that appears to be sent from suspicious senders or has a subject line that appears suspicious, they are advised NOT to open the message. They are advised to contact the I.T. Div. and identify the message for further investigation.

Limitation on the City's Liability
Authorized users use City computer systems at their own risk. The City will not be responsible for legal or financial obligations arising through unauthorized use of City computer systems including, but not limited to, e-mail, Internet, or other electronic communications systems.

Implementation Policy Review
The City will conduct periodic reviews of this policy, which is subject to change at the sole discretion of City management.

See Employee Agreement for Use of Computers, Internet, E-mail, and other Electronic Systems Form located in the "Forms" section of the Employee Handbook.