Office of the Inspector General

Commonwealth of Massachusetts

Gregory W. Sullivan
Inspector General

Advisory for Local Officials: Computer Usage Policies

May 2005

Massachusetts Office of the Inspector General

Address:
Room 1311
John McCormack State Office Building
One Ashburton Place
Boston, MA 02108

Contact Information:
(617) 727 - 9140
(617) 523 - 1205 (MCPPO Program)
(800) 322 - 1323 (Confidential 24-hour Hotline)
(617) 723 - 2334 (FAX)
www.mass.gov/ig

Advisory for Local Officials: Computer Usage Policies

The Office of the Inspector General has prepared this advisory to help local officials understand the importance of appropriate computer usage policies for government owned or operated computers. The Inspector General's office is charged with preventing and detecting fraud, waste, and abuse in state and local government. Whenever possible, we emphasize prevention. This advisory should be used by public officials to create their own computer usage policies or to update any existing policies. All local jurisdictions should have a computer usage policy.

Introduction to Computer Usage Policies

Public employees rely on government owned or operated computers to conduct daily business and to better serve the public. It is important that managers be proactive in educating employees in the appropriate usage of computer systems. Without a clear policy, jurisdictions may not be able to hold employees accountable for system abuses.

Acceptable Uses of Government Owned Computers

Computer usage policies should clearly state that all government owned or operated computer systems should be used only to conduct official business. Employees should be encouraged to use computer resources to the fullest extent in pursuit of your jurisdiction's goals and objectives. This use may include accessing education and research tools via the internet or using properly licensed software.

Your jurisdiction may decide to allow limited, occasional, or incidental personal use of computers including electronic mail and internet access. This use should be clearly defined. Even when occasional usage is permitted, employees should use discretion when using the computer and/or the internet for personal use. Personal use of computer resources should never include:

- violation of any local, state, or federal laws or regulations;
- political, religious, or commercial activity;
- violation of your jurisdiction's personnel regulations;

- sending or receiving of any discriminatory, threatening or harassing messages;
- accessing or sharing of sexually explicit, obscene, or otherwise inappropriate materials;
- violation of any intellectual property rights;
- gaining, or attempting to gain, unauthorized access to any computer or network;
- depleting system resources and/or consuming system resources or storage capacity on an ongoing basis.
- intercepting communications intended for other persons;
- misrepresenting either the jurisdiction or a person's role in the jurisdiction;
- distributing of chain letters;
- accessing online gambling sites; or
- libel or defamation any person.

In addition, your jurisdiction should retain the right to inspect any computer and any files or data sent, received, or stored on that computer in order to supervise, control, and ensure efficient and proper operation of the workplace. Your agency may also choose to monitor any or all network traffic. There should be no expectation of privacy by your jurisdiction's employees. Use of your jurisdiction's computer resources should signify consent for your jurisdiction to monitor and/or inspect any data stored in, sent from, or received by the computer. Your jurisdiction may wish to have an annual audit of a random sample of computers to ensure compliance with policies.

Copyright Protection

Employees should obey intellectual property rights when using computer resources. Not only do legal protections exist for most software programs, but also for text and graphics on a web site.

Proper Use of Electronic Mail

When making use of government electronic mail (i.e. an electronic mail address line or electronic mail message that identifies an employee as an employee of your jurisdiction) consider the electronic mail message to be the equivalent of a letter sent on official letterhead. Many users regard electronic mail as a quick, informal way to communicate,

however electronic mail can be stored, copied, printed, or forwarded by recipients. Therefore users should not write anything in an electronic mail message that they would not feel just as comfortable putting into a memorandum or letter.

In Massachusetts, electronic mail is considered a public record and should be treated as such. Electronic mail is subject to freedom of information requests and the commonwealth's record retention policies.

Portable Computers

Some government employees are provided with portable computers to conduct business when not in the office. The policies listed above should also apply to portable computers owned or operated by the government. Portable computers should only be used to conduct official business. Personal use of portable computers should be limited to the greatest possible extent.

Computer usage policies may define when and where portable computers may be used offsite. For example, work on confidential business should not be conducted in a public place where the work could be seen by others. Additionally, employees using portable computers offsite should be responsible for protecting the computer and any confidential files from theft or security breaches. This may include using a power-on password and encryption software. Any breaches of computer security or theft should be reported to the jurisdiction's designated staff member immediately.

Employees should be aware of the procedures for using both password protection and encryption software before taking a portable computer offsite. Additionally, employees should be familiar with the proper handling of portable computers and diskettes when clearing security gates. Employees should be responsible for recharging the equipment and should report service and maintenance issues to the jurisdiction's designated staff member as soon as possible.

Employee Responsibility

It is the responsibility of public employees to familiarize themselves with their jurisdiction's computer usage policy. Employees should be required by their jurisdiction to sign a form acknowledging that they have read and understand the jurisdiction's computer policy. It should be the employee's responsibility to make sure that they follow these policies.

Management Responsibilities

Local managers should be responsible for establishing a computer usage policy for their jurisdiction and for making all employees aware of their jurisdiction's policies. Managers should also be responsible for:

- Ensuring employee compliance with the policy;
- Keeping track of employee computer usage policy acknowledgment forms if the jurisdiction requires employees to sign one.

Example of Computer Usage Policies

This office has identified the following example of computer usage policies:

- Massachusetts Executive Office for Administration and Finance

  Acceptable Use of Information Technology Resources

  www.mass.gov/Aitd/docs/policies_standards/acceptableuse.pdf