

# ComPuter use policy

|   |   |
|---|---|
| <p>POLICY &amp; PROCEDURE NO.<br/><b>2004-3</b></p>                                 | <p>ISSUE<br/>DATE: 02-29-04<br/>-</p>                                     |
| <p>MASSACHUSETTS POLICE ACCREDITATION<br/>STANDARDS<br/>REFERENCED: <b>none</b></p> | <p>EFFECTIVE<br/>DATE: 02-29-04<br/>_____<br/>Chief Leo A. Sacco, Jr.</p> |
| <p>REPLACES POLICY &amp; PROCEDURE:<br/>2000-4</p>                                  | <p>REVISION<br/>DATE:</p>   |

## **I. Policy**

That all Medford police department personnel use computers, computer applications, computer programs, Internet resources and network/Internet communications in a responsible, professional, ethical, and lawful manner.

## **II. POLICY REVIEW**

This policy will be reviewed by the Computer Operations Unit Commander and the Administrative Captain or any person so designated by the Chief of Police on an annual basis to ensure that it is legally sound and reasonably enforceable.

## **III. POLICY TRAINING**

All full-time officers, administrative staff, support personnel, student interns, volunteer staff and/or any other persons so authorized to use the police department computers will become familiar with and adhere to the provisions of this policy and receive training and notification pertaining to this policy by in-service training, internal mail, email, guard room posting and occasional network log-on reminders.

## **IV. POLICY GUIDELINES**

### **A. Prohibited Behavior/Material**

- 1.** Unless it is directly related to an approved undercover operation or approved ongoing investigation, all Medford Police Department personnel are prohibited from using the department's computers (including personal computers connected to the network or telephone dial-up lines) by knowingly transmitting, receiving and/or storing any offensive communication and/or offensive computer file that is:
  - a.** Discriminatory or harassing;
  - b.** Derogatory to any individual or group;
  - c.** Obscene, sexually explicit or pornographic;
  - d.** Defamatory or threatening;
  - e.** In violation of any license governing the use of software; or copyrighted material.

**2.** That all Medford Police Department personnel are forbidden from disseminating any child pornography or other pornography to anyone by any means either in an online undercover capacity and/or ongoing investigation.

**3.** That all Medford Police Department personnel, upon obtaining approval from the Commanding Officer, or respective Unit Commander, may use the department computers, computer applications and computer programs for limited personal use, ensuring that this use does not interfere with their primary police assignments. All employees are expected to demonstrate a sense of responsibility and not abuse this limited use privilege.

**4.** That all Medford Police Department personnel are hereby informed that there is no expectation of privacy in the computer systems, files, directories, folders or other data storage areas in all of the properties belonging to the Medford Police Department, City of Medford and the North Eastern Massachusetts Law Enforcement Council.

**5.** That all data files, electronic information, data created and/or communicated to and from Medford Police Department personnel using any computer belonging to the Medford Police Department, City of Medford and the North Eastern Massachusetts Law Enforcement Council is subject to occasional audit checks, security assessments and forensic examinations.

**6.** That the Medford Police Department in order to ensure the continuity and safe operations of its network and computer resources under its control will (on occasion), employ intercept, capture and detection programs that search for patterns of abuse, security risks, illegal activity and any violation of this policy.

**7.** Unless otherwise authorized by this policy, that all Medford Police Department members are prohibited from engaging in or attempting to engage in:

**a.** Monitoring or intercepting the files or electronic communications of other employees or third parties;

**b.** Hacking or obtaining access to systems or accounts (internal or external) they are not authorized to use;

**c.** Using other people's network log-in accounts, email addresses and passwords;

**d.** Breaching, testing, or monitoring a computer or tampering with system configuration and/or network security measures.

**e.** Installing any software program, application or hardware without first obtaining authorization from the Computer Operations Unit Commander or his designee.

**8.** That all Medford Police Department personnel should not (unless approved and acting in an undercover capacity) send

e-mail or other electronic communications that can hide the identity of the sender or represent the sender as someone else to include forms of spoofing, masquerading and/or anonymous remailing/WEB surfing services.

**9.** That all Medford Police Department personnel should not abuse programs and/or abuse computer resources that can be used in a manner that is likely to cause major network congestion or significantly hamper the ability of other Medford Police Department personnel to access and use the system;

**10.** That all Medford Police Department personnel should respect and comply with all copyright and software licensing agreements and are forbidden to use, copy, retrieve, modify or forward copyright protected materials except as permitted by law.

**11.** That all Medford Police Department personnel refrain from using encrypted programs and encrypted communications (unless previously approved and/or acting in an undercover capacity). If encrypted programs are used, it would be for the purposes of safeguarding sensitive/confidential information and certain authorized online investigations. Employees who are authorized to use various forms of encryption on files and communication must provide the Computer Operations Unit Commander with a sealed printed copy (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files, including any user accounts and passwords used in accessing secure resources and network configurations.

**12.** That all Medford Police Department personnel restrict access (electronically and/or physically) to their computer systems to ensure adequate security and prevent destruction or tampering with the computers, including computer laptops installed in police motor vehicles.

**13.** That all Medford Police Department personnel conduct a visual and operational inspection on all equipment and media associated with their computer systems and if there appears to be any damage, tampering or malfunctioning of the equipment to report it as soon as possible to the Computer Operations Unit Commander or his designee.

**14.** That all Medford Police Department personnel will not reassemble and/or disassemble computer equipment belonging to the Medford Police Department without express permission from the Computer Operations Unit Commander or his designee.

**15.** That all Medford Police Department personnel are aware of certain State Public Record Laws, which require that any official police department correspondence may fall under “public records” including

government records generated, received, or maintained electronically, including computer records, electronic mail, video and audio tapes (unless it is exempted by law).

**16.** That all Medford Police Department personnel log into the department computers in their designated work areas (on a regular basis) to read and respond to official department emails. All Medford Police Department personnel are required to know their email user names and passwords and are responsible for logging onto and off of their accounts. Furthermore, all Medford Police Department personnel are prohibited from allowing others to use their assigned email/network accounts and/or leave unattended, open access to their email/network accounts.

**17.** That all Medford Police Department personnel have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of the department's computers and that those who abuse the privileges and guidelines set forth in this policy will be subject to corrective action, including but not limited to possible termination of employment, legal action, and criminal liability.