	MEDFIELD POLICE DEPARTMENT	**POLICY NO. 4.22**

INTERNET ACCESS

MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: **11.4.4**	DATE OF ISSUE: 07/02/2023 EFFECTIVE DATE: 07/02/2023 REVISION DATE: 11/03/2025
ISSUING AUTHORITY: Michelle Guerette Chief of Police	

BACKGROUND:

With the use of computers as a communications tool, what took days or weeks to accomplish a few years ago can now take minutes. E-mail, live scan fingerprinting, digitized images, audio and video puts high quality records in the hands of law enforcement officials quickly.

POLICY:

The Town of Medfield owns, operates, and provides computer systems to Medfield Police Department personnel for accessing the internet and Town e-mail accounts. These computers should be used for Department business only. Their use is governed by this policy and the Town of Medfield Network Information Systems (NIS) Security Policy.

PROCEDURES:

1. All Department employees shall be trained in the use of the Town of Medfield external e-mail system. All external e-mail accounts are assigned to specific personnel and are password protected. Each police officer is responsible for his password.

2. Employees shall check their external e-mail at least once every workday. Once an e-mail is received, it shall be understood that the contents of that e-mail, to include attachments, have been formally issued to the employee. It is the responsibility of each employee to review the information within.

3. The Town of Medfield external e-mail system is intended for legitimate Department business. The e-mails of Department employees are considered public record unless the content falls under a statutory exemption.[1] It is unlikely that e-mails containing jokes, obscene images, or personal comments to others will fall under one of the statutory exemptions.

4. Users shall not use NIS internet access to download, upload, store, print, post, or distribute pornographic, obscene, sexually explicit materials, games, or other unacceptable material. Viruses can enter the system via innocent files such as internet images and games, and then wreak havoc on system operability, steal data or passwords, or allow unauthorized users to access the system. Users may visit an otherwise unacceptable site if it is for a legitimate law enforcement investigation, and only with authorization of a supervisor.

5. If an employee accidentally accesses an unacceptable site, the employee must immediately disclose the incident to a supervisor. Such disclosure may serve as a defense against an accusation of an intentional violation of this policy.

6. Employees shall not introduce computer software and data disks into a Department controlled computer systems hardware. This shall include transferring information from any source regardless of its origin.

a. Only authorized software shall be installed on any computer.
b. Only licensed software shall be installed on any computer. **[11.4.4]**

[1] M.G.L. c. 4 s. 7