



New Bedford Police General Order

Subject COMPUTER USAGE POLICY	General Order Number 2-13
Date of Issue 05/28/00	Effective Date 05/28/00
Re-evaluation Date 07/15/19	<input type="checkbox"/> New <input checked="" type="checkbox"/> Amends
C.A.L.E.A.	Cross references

This General Order is designed to provide guidelines for the use of New Bedford Police Department's Computer Equipment, Network, and permitted Use and Access to the Internet. The computers, software, and network they connect to are the property of the City of New Bedford Police Department and may only be used for legitimate police purposes. City of New Bedford Police Department Employees ("Users") are provided access to this equipment, network, and the Internet to assist them in the performance of their duties.

Any User accessing the Internet through the Department's computer resources or connecting to any Department computer equipment through the use of a personal tablet, laptop, cellular phone, portable storage drive or similar device(s), shall complete and sign the "Acknowledgement of Understanding"(see attached) and adhere to the provisions contained in this General Order. Once completed, these forms shall be forward to the Chief's office kept on file and stored.

All Users have a responsibility to use the New Bedford Police Department's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet may result in disciplinary action, including possible termination, and civil and criminal liability.

I. Permitted Use of Internet and the City of New Bedford's Police Department's Computer Equipment and Network

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the internet do so at their own risk and the New Bedford Police Department is not responsible for material viewed or downloaded by users from the Internet. To minimize these risks, your use of the Internet and the computer network at the New Bedford Police Department is governed by the following policy:

II. Computer Network/Equipment Use Limitations

Prohibited Uses. The Department's computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, self-replicating programs, etc.), political material, pornographic text or images, or any other unauthorized materials. Users may not use the Department's Internet connection to download games or any other entertainment software (including screen savers), or to play games over the Internet. Additionally, you may not use the computer network to display, store or send (by e-mail or any other form of electronic communication such as bulletin boards, chatrooms, Usenet groups, etc.) material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful. Furthermore, anyone receiving such materials shall notify their supervisor immediately. The Chief of Police reserves the right to limit or deny computer-network access as defined in this General Order, to employees placed on administrative leave.

System Tampering. Under no circumstances are Users authorized to modify the configuration of any components of the Department's computer network. This includes, but is not limited to, hardware installation, modification to configuration settings, installation of peripherals (i.e. printers, scanners etc.), software installation, equipment relocation, etc. Beyond basic equipment troubleshooting, such as removal of paper jams, no equipment should ever be opened or dismantled in any way by Users and no software should ever be installed or uninstalled by Users.

Illegal Copying. Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to license or download any material without first obtaining the express written permission of the New Bedford Police Department's MIS Division.

Computer/Peripheral Equipment Procurement. All purchases of computer equipment, computer software and computer peripherals such as, but not limited to: personal computers, printers, scanners, digital cameras, modems, soundcards, etc., is expressly prohibited without prior written approval of the Department's MIS Director. The City's Purchasing Agent will not authorize any such purchase without this prior approval. This policy does not apply to consumable supplies such as printer ribbons, toner cartridges, floppy diskettes, computer paper, etc. These items follow standard procurement guidelines of the City's Purchasing Department.

Communication of Trade Secrets. Unless expressly authorized to do so, Users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to the Department. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under state and federal economic espionage laws. Passwords are used by the Department as a means to safeguard access to the Department's networks and information. Under no circumstances should passwords be shared with anyone.

III. Duty not to Waste or Damage Computer Resources

Accessing the Internet. To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to the Department's network must do so through an

approved Internet firewall or other security device. Bypassing the Department's computer network security by accessing the Internet directly by modem or other means is strictly prohibited unless formally in writing authorized by the Department's MIS Division.

Frivolous Use. Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending any amount of time on the Internet for non-business-related business purposes, playing games, engaging in online chat groups, Facebook, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

Virus detection. Files obtained from sources outside the Department, including but not limited to disks, memory sticks, cell phones, tablets brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage the Department's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Department sources, without first scanning the material with Department-approved virus checking software. If you suspect that a virus has been introduced into the Department's network, notify the MIS Division immediately.

IV. No Expectation of Privacy

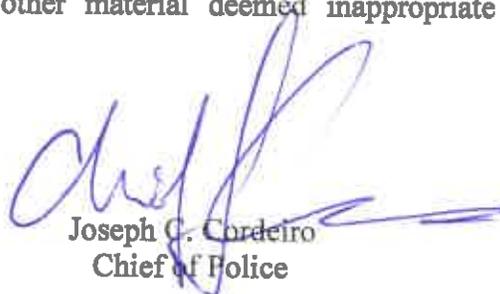
Members of the Department are given computers, e-mail accounts, and Internet access to assist them in the performance of their duties. Users should have no expectation of privacy in anything they create, store, send or receive using the Department's computer equipment. The computer network and everything done with it are the property of the Department and may be used only for Department purposes.

Waiver of privacy rights. Users expressly waive any right of privacy in anything they create, store, send or receive using the Department's computer equipment or Internet access. Users consent to allow Department personnel access to and review of all materials created, stored, sent or received by Users through any Department network or Internet connection.

Monitoring of computer and Internet usage. The Department has the right to monitor and log any and all aspects of its Department's computer systems including, but not limited to, monitoring Internet sites visited by Users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users including e-mail.

Blocking sites with inappropriate content.
The Department has the right to utilize software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

cc: All Divisions and Bureaus
Policy Manual



Joseph C. Cordeiro
Chief of Police

Acknowledgement of Understanding

Name: _____ Employ #: _____

Title: _____

Date: _____

Need Internet Access: Yes No

Need internal E-mail Account: Yes No

I have read and agree to comply with the terms of this policy governing the use of the City of New Bedford's computer equipment and computer network. I understand that violation of this policy may result in disciplinary action, including possible termination and civil and criminal penalties.

Signature

Date

Printed name

Date

Supervisor's signature

Date
