



Newport News Police Department - Administrative Manual

ADM-540 – AGENCY COMPUTER & INFORMATION TECHNOLOGY USAGE

Amends/Supersedes: ADM-540 (06/12/2019)

Date of Issue: 11/15/2021

See Also: Section [1403 Use of Information Technology](#), City Personnel Administrative Manual (PAM)

I. GENERAL

- A. Employees will not make any information technology-related purchases (e.g., computers, monitors, external drives, software, printers, scanners, cameras, audio/visual equipment, or related peripheral devices, subscriptions or purchase of services from third-party providers, etc.) using agency funds, without first consulting with the Public Safety Information Technology (IT) Unit supervisor.
- B. Any employee assigned an agency computer, its related documentation, software, and accessories, whether on a permanent or temporary basis, shall be solely responsible for its care and safekeeping.
- C. *Computer*, as referenced, applies to all electronic resources capable of receiving and sending electronic communication, retrieving or organizing Department information, and connection to the City's WAN. The definition will include but is not limited to MDCs, electronic notebooks, tablets, desktop or laptop PCs, etc.

NOTE: Smartphone use for electronic communications will also fall under any applicable sections (i.e., correspondence, privacy, games, etc.) (See also: [ADM-535 Cellular Phone Use](#))

- D. No department-owned computer equipment shall be moved (e.g., unplugged from the network, removed to another office, etc.) without the prior approval of the system administrator or a representative of the IT Unit.

NOTE: This does not include the temporary undocking of laptops and MDCs associated with normal, daily use.

- E. The use of obscene, profane, discriminatory, demeaning, or degrading language in any electronic correspondence is strictly prohibited.
- F. While on or off-duty, employees will be mindful of sending or receiving e-mails, viewing internet sites or web pages, or engaging in activities related to computers or information technology, potentially bringing the Department into disrepute or discrediting individuals. Employees shall adhere to the PAM section [1000 Standards of Conduct](#), [ADM-210 Standards of Conduct/Disciplinary Action](#), and the Department's Code of Ethics.
- G. Employees shall not use the Department's electronic communications resources for personal gain (e.g., the sale of personal items, homes, services, etc.), whether it is for themselves, family members, or friends.

NOTE: This does not prohibit the e-mail dissemination of information regarding fund-raising and ticket sales for Department-sponsored or sanctioned group events.

- H. Employees shall have no expectation of privacy regarding electronic or physical records, including e-mail, personal files, or official work documents, either received or generated by them while using department-owned electronic resources or connected to a City-approved network. The Department reserves the right to access, without prior notice, any information from any information technology resource. It may require employees to provide passwords to files that are encrypted or password protected upon request.

- 1. Employees will not transmit or receive confidential or sensitive Department information over

their personal non-City messaging platforms (i.e., Google Mail, Facebook, Twitter, Snap Chat, Slack, etc.).

2. Storage of employee personal information on Department computers or peripherals is done at the employee's risk and is subject to City disclosure and surrender requirements.
- I. Department personnel will follow the mandates of the [Virginia Freedom of Information Act](#) (Chapter 37, Title 2.2 of the Code of Virginia) and [ADM-160 Privacy/Dissemination of Information](#), as they relate to the dissemination of information and electronic records when using computer resources in the course of their work activities. [82.1.7]
- J. Connecting personally-owned computer equipment, including peripheral devices such as printers, data storage devices, scanners, *etc.*, to the Department's wide-area network (WAN) is strictly prohibited without documented approval from the employee's chain of command and the concurrence of the IT Unit supervisor (as set out in section II.B.)
- K. Employees shall not use any personally-owned photography, video, or audio recording equipment, digital or otherwise, (e.g., cellular phone, pocket pen camera, digital camera, etc.) to document Department law enforcement-related evidence or investigative photos unless expressly set out in section III. E. of [ADM-535 Cellular Phone Usage](#).
- L. Employees shall observe all copyright and licensing restrictions associated with computer media and software applications.
- M. Personnel accessing Department computer systems shall comply with the general regulations and specific procedures regarding these systems as established, and any rules or regulations issued by the City regarding such systems and their use (See also: PAM section [1403 Use of Information Technology Policy](#). Any employee who violates these policies may be subject to disciplinary action under Department policy and PAM section [1000 City Standards of Conduct](#), resulting in the revocation of access rights to any or all Department computing resources, as determined by the Chief of Police. [82.1.6])

II. PROCEDURES

A. Use of Department Computer Equipment and Peripherals

1. Department computer resources are designed/intended to conduct official business. The installation of games or other software for entertainment purposes is prohibited. Exceptions to official business use include:
 - a. Infrequent personal use is permissible if limited in scope and frequency. Such use may not be connected to for-profit activities or promoting any product, service, or cause that the Chief of Police or designee has not explicitly approved.
 - b. Employees may use departmental computer resources for professional and career development purposes when within this policy and with the prior approval of an appropriate supervisor.
2. The assigned employee is responsible for ensuring their computer's security against unauthorized use. Employees will not allow unauthorized personnel to use their user-ID or passwords to gain access to any department computer, City virtual private network (VPN), NNPd WAN, the City's mainframe systems, the City's e-mail systems, or any other secured system designated for Department business. Employees are responsible for all activities that transpire under their user ID.
3. To avoid breaches of security or theft, employees will utilize the following measures, as applicable:
 - a. Set screen saver passwords;

- b. Close and secure the door to any private office;
- c. Log off of any computer resource when they leave a work area;
- d. Lock their vehicle when left unattended; and
- e. Secure their computer in their residence.

4. Employees are required to log off from all agency computer systems at the end of their workday.

B. Use of Personally-Owned Computer Equipment and Peripherals

[11.4.4]

1. No personally-owned computer equipment or peripherals may be attached to the WAN without prior written consent through the employee's chain of command and the concurrence of the IT Unit supervisor.
2. Employees using any personal device that has received special written approval for attachment to the WAN is subject to network protective action by the Department's or City's IT technicians, including, but not limited to:
 - a. Requiring the device's hardware or software to be upgraded to the requirements of the Department's systems and software before WAN connection, or as a condition of continuing the WAN connection;
 - b. The device (and user) may be subject to some, or all, Department or City policies pertaining to City/Department-owned technology equipment.
 - c. The device may be subject to a data wipe by Department or City IT technicians in a compromised security situation (for example, theft or loss of the device), resulting in the loss of the employee's data.
 - d. The device may be subject to subpoena and the legal discovery process in connection with official use, resulting in a temporary loss of use or possession.
3. The IT Unit is not responsible for responding to any hardware or software support issues relating to personally-owned computer equipment or peripherals.
4. In all cases where personally-owned computer equipment or peripherals are used in Department workspaces, the equipment owner shall assume complete and sole responsibility for the equipment's legal and safe operation and any liability that may result from its presence or use on or in city property.
5. Neither the City nor the Department shall be liable for any personally-owned computer equipment, software, or peripheral devices that may be stolen, damaged, or otherwise made inoperable while in Department workspaces.
6. Any media (i.e., USB drives, external HD, DVDs, CDs, *et cetera*) not owned or supplied by the Department, and which has, or is intended to be, used with any device will be scanned before transferring any files into a Department computer.

NOTE: Employees wishing to upload information into a Department-owned system must contact the IT Unit so the media may be virus scanned.

7. If Department or City computer equipment becomes infected with a virus, and the infection is traced to a personally-owned computer system or media device, the individual transferring the virus to the system may be held liable for the costs of removing the virus.

C. Accountability and Auditing

[C6.8.5, L82.1.6(d)]

1. The IT Unit will perform a documented quarterly audit of all computer systems for verification of passwords, access codes, and user accounts for possible violations and improper use, including the: [T7.3.5]

- a. Verification of all user accounts on all computer platforms currently in use by employed users or to ensure that all such accounts for former employees have been disabled. [T7.3.7(b)]
 - b. Verification of password protection on all user accounts to include minimum password lengths of eight characters to include, at a minimum: (1) at least one capitalized letter, and (2) one number or unique character. [T7.3.7(a)]
 - c. Reviewing all permissions to verify that users may access only the information required to perform their duties as approved by supervision. [T7.3.7(b)]
 - d. Review of any other security measures, as appropriate.
2. Personnel will change their system password every 90 days when logging into the network. [T7.3.8]
 3. The system administrator will ensure that the internal inventory records for all departmental computer resources are kept current and available for inspection.

D. System Backups

[82.1.6(a,b)]

1. The system administrator will ensure that all dynamically changing computer files are backed up daily to a secure location with an active, non-corrosive fire suppression system. Daily incremental backup tapes will be stored in a climate-controlled, secure area. [T7.3.6(a)]
2. The system administrator shall ensure that the agency's complete data storage system is backed up no less than weekly. Weekly backup tapes will be stored in the climate-controlled, secure concrete building located off-site. [T7.3.6(b,c)]
3. Requests to review or restore data from backup tapes or stored computer files shall be made in writing to the system administrator. [T7.3.6(a,c)]
4. Computer files ported to tape for backup purposes shall remain viable and retrievable for up to six months. At that time, the backup tapes will be overwritten and reused. [T7.3.6(d)]

NOTE: The amount of online storage shall be increased, as necessary, to ensure that all active user files shall remain available and accessible on the agency's network, regardless of the agency's backup capability.

E. Importing/Downloading Information and Software

[11.4.4; 41.3.7(a,b)]

1. The IT Unit will approve all software loaded onto Department computers or provided through cloud access.
- NOTE:** Software includes any which enables the user to perform tasks using computer resources (i.e., any programs, routines, scripts, applications, firmware, grayware, freeware, open-source, sound and video files, attachments to e-mails, Internet files, or other external sources) whether cloud-based or requiring a hard installation.
2. Employees requesting to purchase and load software onto Department computers will consult with their supervisors, then the IT Unit to ensure that the software does not interfere with other programs and systems.
 3. All software loaded into a system will be inventoried for maintenance of the license record in the Planning & Information Technology Division. The software will be licensed to the "Newport News Police Department."

III. Mobile Data Computers (MDCs) and Similar Mobile Technology

[41.3.7]

- A. MDCs (and similar mobile technology) provide the ability to communicate and retrieve routing information, allowing Communications personnel to deal with more urgent calls. Officers shall use this technology unless in extenuating circumstances.

NOTE: As used, the term "MDC" also refers to tablets or similar mobile devices.

- B. All personnel operating a vehicle equipped with an MDC shall comply with the general computer rules and regulations and specific procedures regarding the use and care of the MDCs, as provided to them. Non-compliance will be brought to the attention of the officer's supervisor for corrective action.
- C. Dispatcher-provided voice instructions shall take precedence over information forwarded and displayed on the MDC.
- D. All MDC entries, including e-mails, talk messages, and conference messages, are recorded and electronically saved, falling under the Commonwealth of Virginia's Freedom of Information Statutes, for review by the Department, the public, and the media.
- E. Officers will observe proper MDC safety use protocol and will not compromise their safety or the safety of others (e.g., do not type while driving, do not perform an NCIC/VCIN check while trying to initiate a traffic stop, *et cetera*).

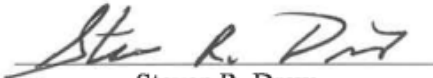
IV. Social Media and Social Networking Sites (PAM section [1410 - Social Media Policy](#))

A. Development of Personal Webpages, Social Media Sites, And Social Networking Sites

- 1. Personnel will not portray themselves as representatives of the Department, the City, or its affiliated programs on their personal webpages, Facebook account, Twitter messages, or any other social media or networking sites without the express written permission of the Chief of Police or designee.
- 2. For safety reasons, employees are cautioned not to disclose their employment with the Department or post any information about any other agency member without that individual's permission.

B. Development of Agency Webpages, Social Media Sites, And Social Networking Sites

- 1. The City Communications Department shall approve all Department social media sites or webpages after receiving approval from the Chief of Police or designee before being posted for viewing.
- 2. Any such site, blog, or webpage used to promote the City or the agency shall clearly indicate:
 - a. They are maintained by the City and prominently display City contact information;
 - b. The City's posting policy regarding appropriate content, if applicable for the social media type. Posted comments will be monitored for adherence to the posting policy, and violating content may be removed, rejected, deleted, or disabled;
 - 1) Content removed from a social media site shall be retained according to Virginia Records Retention requirements; along with
 - 2) A description of the reason the content was removed.
 - 3) That any opinions expressed by visitors to the site(s) do not necessarily reflect the opinions of the Newport News Police Department or the City of Newport
 - c. Any content posted or submitted for posting is subject to full public disclosure (i.e., FOIA, e-discovery), storage, and media management laws.
 - d. Questions regarding the appropriateness of a prospective post shall be made before posting to the employee's supervisor or the Department's Public Information Office.


 Steven R. Drew
 Chief of Police