
**Section: TWO
Chapter: SEVEN**

SUBJECT: Employee Computer, Internet and Electronic Mail Policy
ISSUE DATE: 08-15-16
REFERENCE: 55.1 & 55.4

I. PURPOSE

As part of this Village of Palmyra commitment to the utilization of new technologies the Village recognizes the Internet and World Wide Web (WWW) as business tools that will enhance our employees' knowledge and productivity while furthering the quality of services provided to the citizens of the Village of Palmyra. In order to ensure compliance with existing copyright and decency laws, and to protect the Village of Palmyra from being victimized by the threat of viruses or hacking into our systems, the following policy has been established.

II. POLICY

The Village of Palmyra may utilize software and hardware monitoring devices that can examine and record all Internet usage. Be aware that the security systems are capable of recording (for each user) each World Wide Web (WWW) site visit, each chat, newsgroup or email message, and each file transfer into and out of our internal networks. The Village of Palmyra reserves the right to utilize available monitoring systems at any time. No employee should have any expectation of privacy as to his/her Internet usage. The department heads and/or network administrators may review Internet activity and analyze usage patterns. Internet resources are devoted to maintaining the highest levels of productivity.

III. INTERNET

- A. The Village of Palmyra reserves the right to inspect any and all files stored in private areas of our network in order to assure compliance with this policy.
- B. Employees will not access inappropriate sites. Inappropriate sites are sites that are clearly not used for management-approved business purposes.
- C. The display of any kind of sexually explicit images or documents on any Village system is a violation of the Village policy on sexual harassment.
 - 1. Sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.
 - 2. If an employee finds himself or herself incidentally connected to a site that contains sexually explicit or offensive material, the employee must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program. (Exception: Police Officers while in the performance of their duties for investigative purposes.)
- D. The Village of Palmyra internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation,

or the laws and regulations of any state, city, Village, province or other local jurisdiction in any material way.

- E. Any software or files downloaded via the Internet into the Village networks becomes the property of the Village of Palmyra. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.
- F. No employee may use Village of Palmyra facilities knowingly to download or distribute pirated software or data.
- G. No employee may use the Village's internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
- H. No employee may use the Village's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
- I. Each employee using the internet facilities of the Village of Palmyra will identify himself or herself honestly, accurately and completely (including affiliation and function where requested) when participating in work-related chats or newsgroups, or when setting up accounts on outside computer systems. (Exception: Police Officers while in the performance of their duties for investigative purposes.)
- J. Only those employees or officials who are duly authorized to speak to the media or in public gatherings on behalf of the Village of Palmyra with respect to their official duties may speak/write in the name of the Village of Palmyra in any Internet transaction.
 - 1. With approval of the Chief of Police, employees may participate in work-related newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves.
- K. Use of Village of Palmyra Internet access facilities to commit infractions such as misuse of Village assets or resources, harassment*, unauthorized public speaking and misappropriation or theft of intellectual property is also prohibited by the policy of the Village of Palmyra.
 - * Harassment:
Those perceived to be offensive or harassing in statement or language including disparagement of others based on their race, national origin, sex, sexual orientation, age, religious, or political beliefs.
- L. Employees may use their Internet facilities for non-business research or browsing during meal time or other breaks, or outside of work hours, provided that all other usage policies are adhered to.
- M. Employees with Internet access may not use Village Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.
- N. Only those Internet services and functions with documented business purposes for the Village of Palmyra will be enabled at the Internet firewall.

IV. TECHNICAL

- A. User IDs and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource must keep that password confidential. Village policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites.

V. SECURITY

- A. The Village has installed security systems to assure the safety and security of the Village's networks. Future security devices may be installed at any time without prior notice.
- B. Any individual who attempts to or successfully disables, defeats, circumvents and/or tampers with any Village owned or controlled personal computer, server, network or other component (including software) will be in violation of N.Y.S. Penal Law § 156 and may be prosecuted, as such, under the laws of New York State.

VI. E-JUSTICE

- A. The New York State Division of Criminal Justice Services' (NYS DCJS) "eJustice" system will be accessed and utilized only by authorized personnel, and will be used only for legitimate Departmental investigations and official police business. The information retrieved from eJustice is not public, and shall not be viewed or shared with any unauthorized person.
- B. All authorized personnel will use the eJustice system in accordance with the "Use and Dissemination Agreement" with NYS DCJS.
- C. Personnel will only access the eJustice system from Departmental computers. Access to the eJustice system from personal computers is prohibited, unless authorized by the Chief of Police in exigent circumstances.
- D. Unauthorized access to, or use of, the eJustice system will result in disciplinary action and/or criminal charges.

VII. FLASH DRIVES

- A. Flash drives (thumb drives) are Agency property and are issued for the convenience of Departmental personnel, and are to be utilized only for official police business. Unauthorized data is not to be stored on, or transferred to or from, the Department-issued flash drive.

IX. SOCIAL NETWORKING SITES

- A. Employees of the Palmyra Police Department have a right to have personal web pages or sites. Social networking sites on the Internet provide people with a portal for connecting with others, sharing information and the opportunity to express their creativity. Some officers choose to make extensive use of online profiles, photographs, videos and blogs. As such, there is the need for personal accountability. Employees of the Palmyra Police Department are prohibited from posting, transmitting and/or disseminating to any personal or social networking website or webpage or other public forum to include text messaging, any of the following:

1. Any photographs, video or audio recordings, likenesses or images of department logos, emblems, uniforms, badges, patches, marked vehicles, equipment, or other material that specifically identifies the Palmyra Police Department, without the permission of the Chief of Police.
2. Representing themselves, directly or indirectly, as a member of the Palmyra Police Department, either by text, photograph, or image depicting the uniform, badge, or patch, in any manner that reflects a lack of good moral character.
3. Representing themselves as an employee of the Palmyra Police Department with other information, opinion, or posture that would bring unfavorable criticism or embarrassment upon the Department.
4. Posting photographs or other depictions of department uniforms, badges, patches, or marked units without permission from the Chief of Police.
5. Posting photographs of the inside of the police facility, as well as any crime, accident or incident scene.
6. Posting of official department training, activities, or work-related assignments and/or material without permission from the Chief of Police.
7. Posting photos, comments, etc. of other department employees without approval from the employee(s).
8. Posting any material that brings discredit to or may adversely affect the efficiency or integrity of the Palmyra Police Department.
9. Posting any material that may jeopardize the safety of any employee.

By the Order of:

David B. Smith
Chief of Police