

# GENERAL ORDER

## PORT WASHINGTON POLICE DEPARTMENT

SUBJECT: <b>DEPARTMENT INTERNET &amp; EMAIL ACCESS AND USE</b>		NUMBER:	1.10.1
		ISSUED:	3/31/09
SCOPE:	All Police Personnel	EFFECTIVE:	3/31/09
DISTRIBUTION:	General Orders Manual	<input checked="" type="checkbox"/> RESCINDS	30.2
		<input type="checkbox"/> AMENDS	
REFERENCE:		WILEAG 3 <sup>RD</sup> EDITION STANDARDS: N/A	

**INDEX AS:**     Email Usage  
                       Equipment, Materials or Property  
                       Internet Usage  
                       Public Property

**PURPOSE:** The purpose of this Order is to define the parameters within which police department employees may use department internet and email services, in executing business activities.

This Order consists of the following numbered sections:

- I.    DEFINITIONS
- II.   INTERNET USAGE
- III.  EMAIL USAGE

I.    DEFINITIONS

- A.   Department: refers to the City of Port Washington Police Department.
- B.   Email: refers to an electronic mail system that creates stores and forwards information using telecommunication links between computer terminals, work stations, servers, or personal computers.
- C.   Information Systems Manager: refers to the individual employee and/or Information Technology Service vendor designated by the Chief to oversee the department's Information Technology system(s).

## II. INTERNET USAGE

- A. It is the policy of the City of Port Washington Police Department to provide Internet services for its employees to enhance their professional activities, improve public communication, and provide superior customer service. Efficient use of the Internet for research and communication will improve the quality, productivity, and general cost effectiveness of department functions.
1. The services provided include accessing various information resources found on the World Wide Web and enabling employees to gain the level of expertise necessary to provide knowledgeable service to an increasingly sophisticated customer base.
  2. The Department's Internet access is a privilege and the Department encourages creative, professional use that enhances productivity.
- B. General Guidelines
1. Internet access is provided as a business tool. When accessing the Internet using Department equipment and/or on Department property, employees shall limit all usage to job-related purposes. The Department expects employees to conduct themselves honestly and appropriately.
  2. A wide variety of information is available on the Internet, some uncensored and unrestricted. The Department does not permit access at any time to materials that may be found offensive or pornographic, nor is the Department responsible for the content of any Internet site.
  3. Employees accessing the Internet are representing the Department. Therefore, all actions and communications shall be conducted in a manner that is consistent with the professional and courteous behavior that is expected of all department employees.
  4. The transfer of information via the Internet is not secure. The confidential nature of Department information must be considered paramount. Therefore, transmittal of confidential information via the Internet is inappropriate and shall not be permitted.

5. Internet use and communication by employees on Department equipment at all times is public and not confidential or private. The Department reserves the right to monitor Internet activity by employees without prior notification. Employees have no privacy with respect to their access or use of the Internet.
6. Under federal and state law, and Department policy, email and electronic files obtained via the Internet are public records and subject at all times to inspection by the public and management in the same manner that paper documents of a similar nature are preserved and made available.
7. Many of the sites on the Internet can be breeding grounds for computer viruses. If these viruses are downloaded, they can cause data and system corruption. Therefore, all downloaded files must be checked for viruses and comply with instructions and directives issued by the Information Systems Manager.
8. No software or hardware may be temporarily or permanently loaded or programming performed by any employee or other person to any Department personal computer or component of the Department's information system without the express knowledge and permission of the Information Systems Manager.
9. The safety and security of the Department's network and resources shall be considered paramount when using the Internet. User passwords are confidential. It is the user's responsibility to maintain the confidentiality of their passwords.
10. Employees shall abide at all times by all guidelines of this policy, and any amendments that may occur from time to time.
11. All use of the Internet shall be in compliance with all federal, state, and local laws and policies, including, but not limited to, those pertaining to property protection, privacy, and misuse of Department resources, sexual harassment, information security, and confidentiality. Access to the Internet provided by the Department shall not be used for any illegal, improper, unprofessional, or illicit purpose or for personal or financial gain.
12. In addition to the parameters outlined in this policy, employees shall use the Internet in accord with the direction of the Chief of Police or his designee.
13. Police department employees may not download and/or install the following types of programs:
  - a) Executable Files, or Files with Extensions of .exe, .com, bat.

- b) Media Players or Real Players
- c) Software to Play Online Music, Streaming Audio, Streaming Video, or Radio Stations.
- d) Chat or Messaging Software
- e) Stock or News Tickers
- f) Screen Savers

C. User Authorization

- 1. The Department encourages Internet use to enhance one's job performance and improve the efficiency and effectiveness of public service. Therefore, the Chief of Police and the Information Systems Manager will coordinate Internet access for department employees.

D. Violation Of Policy

- 1. Violation of this policy shall be regarded as a work rule violation. Failure of an employee to adhere to and comply with these policies may result in disciplinary action up to and including discharge of employment with the City of Port Washington Police Department.

III. EMAIL USAGE

- A. It is the policy of the City of Port Washington Police Department to provide email access and accounts for employees as a communication tool in order to conduct Department business.

B. General Guidelines

- 1. Email accounts are provided for official Department business only and shall not be used for personal reasons except in the case of an emergency or specific personal business that cannot be conducted during non-working hours, and shall not be used for e-commerce, to conduct a business, or for any other personal or financial gain. Work duties shall take precedence over personal business.
  - a) The Department expects employees to conduct themselves honestly and appropriately.
  - b) Employees shall not abuse this privilege.

2. The email system is maintained by the Department on Department equipment and at all times is public and not confidential or private. The Department provides email as a business tool. Therefore, the Department reserves the right to monitor email messages without prior notification for the purpose of maintaining and supporting the Department email system. Employees have no privacy with respect to their access or use of the email system.
3. The use of email for any illegal or unethical activities, or activity, which could adversely affect the Department, is prohibited.
4. Various information sources can be accessed through email including list serves, forums, and discussion groups. Participation for business purposes is encouraged. However, approval by the Chief of Police is required before any associated costs or charges are incurred.
5. Use of email and construction of messages must be consistent with the professional and courteous behavior that is expected of Department employees. If participating in forums, postings or list serves employees must recognize their representation of the Department and the confidentiality of Department business.
6. No person without specific authorization shall read, alter or delete any other person's computer files or email.
7. Under federal law, email and electronic files obtained via the Internet are public records and subject at all times to inspection by the public and management in the same manner that paper documents of a similar nature are preserved and made available.
8. Email messages and the transfer of information are not secure. Confidential information shall not be transmitted through email and shall not be permitted.
9. Email attachments can be breeding grounds for computer viruses. If these attachments are opened, they can cause data and system corruption. Therefore, all attachments must be checked for viruses and comply with instructions and directives from the Information Systems Manager.
10. Employees shall abide at all times by all guidelines of this policy, and any amendments that may occur from time to time.

C. User Authorization

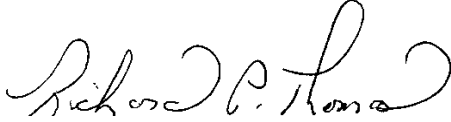
1. The Department encourages email use to increase business communications and enhance one's job performance. Therefore, the Chief of Police and the Information Systems Manager will coordinate email account access for employees.

D. Violation Of Policy

1. Violation of this policy shall be regarded as a work rule violation. Failure of an employee to adhere to and comply with these policies may result in disciplinary action up to and including discharge of employment with the City.

**APPROVED:**

**DATE:**



3/31/09

---

Chief Richard P. Thomas