


HAVERFORD TOWNSHIP POLICE DEPARTMENT OPERATIONS MANUAL		
Issue Date February 2021	Review Date February 2022	Directive Number 6.5.4
Accreditation Index:		Rescinds: Directive 6.5.4 of November 2019
Chapter: Six – General Procedures		Section: Five – Communications and Information Technology
Chief of Police: <i>John F. Viola</i>		

SUBJECT: INFORMATION TECHNOLOGY SYSTEMS

I. PURPOSE

The purpose of this Directive is to establish guidelines for the proper use of business equipment including, but not limited to, all information technology systems, computers, electronic mail, voice mail, internet access, and all other record management systems of the Haverford Township Police Department.

II. POLICY

The Department has installed information technology systems such as computers, electronic mail, and voice mail to assist Department personnel in working more efficiently and effectively. This policy is designed to provide regulations for the proper use of these information systems.

All information stored in the information technology systems of the Department, whether stored electronically, manually or in any other format is the property of the Haverford Township Police Department.

III. DEFINITIONS

Information Technology Systems – For purposes of this Directive these systems shall include the following:

Computers – all hardware and software systems which are the property of the Department whether connected to the network or as a stand-alone personal computer (PC), and all information stored on these computer systems.

Digital Media Storage Devices - All storage mediums associated with computers, tablets, cameras, phones, etc. such as hard drives, compact discs, external hard drives, flash drives, thumb drives, SD or Micro SD cards, or any similar devices capable of retaining information or data.

Electronic Mail (e-mail) – electronically transmitted or received information using the Department’s e-mail system both internally and on the internet.

Information Technology Department (I.T. Department) – Is the Township Department responsible for all aspects of Information Technology services for all Haverford Township government departments and officials, including the Police Department.

Information Technology Director – Is the Township Department head of the Information Technology Department. The I.T. Director is the authorized person designated by the Township Manager and the Chief of Police to manage all Information Technology systems utilized by the Police Department.

Instant Message or Text – a written form of instant digital communication that also allows for the transmission and reception of audio and video files and images.

IP telephony services including Video Conferencing and VoIP – communication methods that allows two or more participants at different sites using computer networks to transmit text, audio and/or video data as well as shares files. (Examples: WebEx, Zoom and more personal services like Skype, Yahoo Instant Messenger, etc.)

Records Management Systems – All records storage and retrieval systems, whether functioning electronically, manually or by any other method of operation used by the Department to store and retrieve information.

Systems Administrator – the person designated by the Information Technology Director responsible for maintaining and upgrading the information technology systems of the Police Department.

Voice Mail – telephonically transmitted or received information stored on the software of the Department’s voice mail system.

IV. PROCEDURES

A. Regulations

1. Department personnel are provided passwords or codes to restrict access to computers, voice mail and e-mail systems.
 - a) These passwords or codes provide a measure of security against unauthorized access to information stored in the systems.

- b) Personnel shall only access files to which they have been granted authority.
 - c) It is the responsibility of all personnel to protect the integrity of these information systems by protecting their passwords or codes.
 - d) Passwords and codes are electronic signatures assigned to a specific employee.
 - (1) Employees shall not disclose their password or code to any person except the Chief of Police, the Information Technology Director or their designee.
2. Employees shall notify the I.T. Department as soon as possible if their password has been compromised.
 3. The Chief of Police and the Township Information Technology Director or their representatives reserve the right to monitor and inspect all Township owned or operated information technology systems, devices and media including but not limited to voice mail and e-mail messages for compliance to these regulations.
 - a) These I.T. devices include but are not limited to the contents of computers, tablets, phones, cameras, digital media storage devices, voice mail and e-mail.
 - b) This monitoring may occur in the course of an investigation indicating unacceptable use of these information systems or as necessary to locate needed information that is not more readily accessible by some less intrusive means.
 - c) Employees shall have no expectation of privacy concerning any business or personal information stored on Department information technology systems.
 4. All material generated by department information technology systems including but not limited to computer, voice mail, e-mail, and all interoffice communication should be treated as confidential by other employees and accessed only by the intended recipient.
 - a) Information stored on Department information technology systems including but not limited to computers, voice mail, and e-mail, properly obtained for some legitimate business purpose, may be disclosed by the Department when necessary to comply with court proceedings or other business necessity.
 5. The following unauthorized uses of Department I.T. systems and devices including but not limited to, computers, voice mail and e-mail are strictly prohibited:

- a) Use to solicit for commercial ventures, religious or political causes, outside organizations, or other non-job related solicitations.
 - b) Use to create, disseminate or store any offensive or disruptive messages.
 - (1) Examples of offensive messages are:
 - (a) messages which have sexual implications, racial slurs, gender-specific comments, messages offensively addressing someone's age, sexual orientation, religion, political beliefs, national origin, or disability.
 - c) In addition, neither the e-mail nor any other department information technology system shall be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization by the Chief of Police or his designee.
 - d) Pornography or any material (visual or sound) that could be offensive under the Township Improper and Sexual Harassment Policy (Directive 1.8.2) shall not be stored on Department digital media or hardware.
 - (1) Accessing web sites, newsgroups, and e-mail that contains similar material is also governed by this Directive and prohibited unless expressly authorized by the Chief of Police or his designee for investigative purposes.
6. Incidental personal use of the Department's computers is permitted, however the Department may, at any time, monitor the personal use of all information technology systems.
- a) Employees shall not have any expectation of privacy with respect to personal information created, edited, viewed or stored on Department information technology systems. These systems include but are not limited to computers, tablets, phones, cameras, e-mail, voice mail or any digital media storage devices, etc
- B. Use of Department Hardware and Information Technology Systems including but not limited to Computers, Tablets, Phones and MDTs.
- 1. No program, file, application shall be uploaded from or downloaded onto any Department owned or operated Information Technology system, device or computer without prior approval of the Chief of Police and the Director of Information Technology.

2. No software shall be loaded onto or used on a Department computer, device or server without prior approval from the Chief of Police and the Director of Information Technology.
3. All activity on department information technology systems should be mission related. The use of the Internet by Department account(s) or through a private account(s) in the work place shall only be used for job related matters or incidentally as described above in section A6.

C. Information Technology Systems Investigative Use and Requirements

1. If there is a legitimate investigative need for offensive material to be viewed, accessed, or placed on the Department's Information Technology System, prior approval shall be obtained from the Chief of Police through the proper chain of command.
 - a) The Information Technology Director shall be contacted so an appropriate I.T. system can be utilized to complete the investigation without compromising the department's security or the investigation.
2. The investigation shall be documented as an official investigation.
 - a) A log of all sites and downloads shall be maintained.
 - b) All files, images, etc. obtained through the investigation shall be maintained as evidence in accordance with Directive # 3.5.2

D. Duty to Access E-mail.

1. It shall be the responsibility of every member of the Department to open their Department e-mail every day they work to ensure they read and comply with all new memorandums, policies, procedures, general orders, or directives that have been issued.

E. Violations

1. Any employee who violates this Directive or uses the information technology systems for improper purposes shall be subject to discipline, up to and including termination.

BY ORDER OF THE CHIEF OF POLICE