	HARRISONBURG POLICE DEPARTMENT General Orders	**Policy Number:** 318
	Chapter: General Operations	**Total Pages:** 7
	Section: Information Technology Use/Electronic Mail	**Issue Date:** 07/02/2021
	Issued By: Kelley Warner, Chief of Police	**Effective Date**: 06/17/2024
	Replaces: All General Orders Previously Issued Relative to Subject	
VALEAC Standards: OPR.01.06 (a), OPR.01.06 (c)		

A. POLICY AND PURPOSE

The purpose of this policy is to provide guidelines for the proper use of department information technology resources, including computers, electronic devices, hardware, software and systems. This policy also establishes guidelines for the proper use and application of electronic mail (email) and Personal Communications Devices (PCD's).

It is the policy of the Harrisonburg Police Department that employees shall use information technology resources, including computers, software and systems that are issued or maintained by the Department in a professional manner and in accordance with this policy. Employees shall also utilize email and other telecommunications devices in a professional manner in accordance with this policy and current law.

Reference City policy:
http://citycentral.harrisonburgva.gov/sites/default/files/it/files/Network_Acceptable_Use.pdf

B. ACCOUNTABILITY STATEMENT

All employees are expected to fully comply with the guidelines and timelines set forth in this policy. Responsibility rests with the supervisor to ensure that any violations of policy are investigated and appropriate training, counseling and/or disciplinary action is initiated. This directive is for internal use only and does not enlarge an employee's civil liability in any way. It should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violation of this directive, if proven, can only form the basis of a complaint by this department, and then only in a non-judicial administrative setting.

C. DEFINITIONS

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented, or licensed by the Harrisonburg Police Department that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department or department funding.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones (including cellular and satellite), pagers, modems or any other tangible computer device generally understood to comprise hardware.

Personal Communication Devices (PCDs) - Includes all mobile telephones, personal digital assistants (PDAs), wireless capable tablets and similar wireless two-way communications and/or portable Internet access devices. PCD use includes, but is not limited to, placing and receiving calls, text messaging, blogging and micro blogging, emailing, using video or camera features, playing games and accessing sites or services on the Internet.

Software - Includes, but is not limited to, all computer programs, systems, and applications, including shareware. This does not include files created by the individual user.

Temporary file, permanent file or file - Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

D. PRIVACY EXPECTATION

Employees forfeit any expectation of privacy with regard to emails, texts or anything published, shared, transmitted or maintained through file-sharing software or any Internet site that is accessed, transmitted, received or reviewed on any department computer system.

The Department reserves the right to access, audit and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received, or reviewed over any technology that is issued or maintained by the Department, including the department email system, computer network and/or any information placed into storage on any department system or device. This includes records of all keystrokes or Web-browsing history made at any department computer or over any department network. The fact that access to a database, service or website requires a username or password will not create an expectation of privacy if it is accessed through department computers, electronic devices, or networks.

E. RESTRICTED USE

Employees shall not access computers, devices, software, or systems for which they have not received prior authorization or the required training. Employees shall immediately report unauthorized access or use of computers, devices, software, or systems by another member to any supervisors.

Employees shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless authorized by that individual to do so.

a. SOFTWARE

Employees shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes, in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any department computer. Employees shall not install personal copies of any software on any department computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the information systems technology (IT) staff and with the authorization of the Chief of Police or the authorized designee.

No employee shall knowingly make, acquire, or use unauthorized copies of computer software that is not licensed to the Department while on department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved employees to severe civil and criminal penalties.

Introduction of software by employees should only occur as a part of the automated maintenance or update process of department or City-approved or installed programs by the original manufacturer, producer, or developer of the software. Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

b. HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to department-related activities. Data stored on or available through department computer systems shall only be accessed by authorized employees who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or department-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

c. INTERNET USE

Internet access provided by or through the Department shall be strictly limited to department-related activities. Internet sites containing information that is not appropriate or applicable to department use and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, gambling, chat rooms, and similar or related Internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member's assignment.

Downloaded information from the Internet shall be limited to messages, mail and data files.

d. TELECOMMUNICATIONS

Telecommunications (telephones, cell phones, texting, email, or other associated platforms and devices) shall be used prudently and in moderation while on duty.

Incidental personal use by employees of the City's communications services and equipment shall be allowed as long as the use does not interfere with the employee's work or the City's operations and does not violate any City policies.

Reference city policy on CityC^2Central:

http://citycentral.harrisonburgva.gov/sites/default/files/hr/Policies/Section%2012%20-%20City%20Communications%201-12.pdf

http://citycentral.harrisonburgva.gov/sites/default/files/hr/Memorandums/%2321HRPM%20-%20Telephone%20Usage.pdf

e. RESTRICTIONS ON USE OF EMAIL

Messages transmitted over the email system are restricted to official business activities or shall only contain information that is essential for the accomplishment of business-related tasks or for communications that are directly related to the business, administration or practices of the Department.

The City provides all employees with a voicemail and an email account. In order to ensure the best possible service and communication between members of the public, between co-workers, and to prevent excessive buildup of either the voicemail or email account, all employees shall check both accounts at least once daily during the employee's scheduled work shift. Emails and phone messages should be addressed in a timely manner.

Sending derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing or any other inappropriate messages on the email system is prohibited and may result in discipline.

Email messages addressed to the entire Department are only to be used for official business-related items that are of particular interest to all users. In the event that a employee has questions about sending a particular email communication, the employee should seek prior approval from a supervisor in his/her chain of command.

It is a violation of this policy to transmit a message under another employee's name or email address or to use the password of another to log into the system unless directed to do so by a supervisor. Employees are required to log off the network or secure the workstation when the computer is unattended. This added security measure will minimize the potential misuse of a employee's email, name or password. Any employee who believes his/her password has become known to another person shall change their password immediately.

F. PROTECTION OF SYSTEMS AND FILES

All employees have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care, and maintenance of the computer system.

Employees shall ensure department computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, logon information and other individual security data, protocols and procedures are confidential information and are not to be shared. Password length, format, structure and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor.

It is prohibited for a employee to allow an unauthorized user to access the computer system at any time or for any reason. Employees shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a supervisor.

G. INSPECTION AND REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Department involving one of its employees or a member's duties, an alleged or suspected violation of any department policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download, or otherwise obtain any and all temporary or permanent files residing or located in or on the department computer system when requested by a supervisor or during the course of regular duties that require such information.

H. EMAIL RECORD MANAGEMENT

Email may, depending upon the individual content, be a public record under the Virginia Freedom of Information Act (VFOIA) and must be managed in accordance with the established records retention schedule and in compliance with state law.

The Custodian of Records shall ensure that email messages are retained and recoverable as outlined in the Records Maintenance and Release Policy.

I. PERSONAL COMMUNICATION DEVICES (PCD'S)

The Harrisonburg Police Department allows employees to utilize department issued PCDs and to possess personally owned PCDs in the workplace, subject to certain limitations. Any PCD used while

on-duty or used off-duty in any manner reasonably related to the business of the Department, will be subject to monitoring and inspection consistent with the standards set forth in this policy.

The inappropriate use of a PCD while on-duty may impair officer safety. Additionally, employees are advised and cautioned that the use of a personally owned PCD either on-duty or after duty hours for business-related purposes may subject the employee and the employee's PCD records to civil or criminal discovery or disclosure under the Virginia Freedom of Information Act.

Employees who have questions regarding the application of this policy or the guidelines contained herein are encouraged to seek clarification from supervisory staff.

a. PRIVACY EXPECTATION

Employees forfeit any expectation of privacy with regard to any communication accessed, transmitted, received or reviewed on any PCD issued or funded by the Department and shall have no expectation of privacy in their location should the device be equipped with location detection capabilities.

b. DEPARTMENT-ISSUED PCD

Depending on a employee's assignment and the needs of the position, the Department may, at its discretion, issue a PCD for the employee's use to facilitate on-duty performance. As such, personal use should be kept to a minimum and/or discouraged if other means of communication are available. Such devices and the associated telephone number, if any, shall remain the sole property of the Department and shall be subject to inspection or monitoring (including all related records and content) at any time without notice and without cause.

c. PERSONALLY OWNED PCD

Employees may carry a personally owned PCD while on-duty, subject to the following conditions and limitations:

a. The Department accepts no responsibility for loss of or damage to a personally owned PCD.
b. The PCD and any associated services shall be purchased, used and maintained solely at the employee's expense.
c. The device should not be used for work-related purposes except in exigent circumstances (e.g., unavailability of radio communications, photos during emergency incidents, etc.). Employees will have a reduced expectation of privacy when using a personally owned PCD in the workplace and have no expectation of privacy with regard to any department business-related communication.
d. If the PCD is carried on-duty, employees will provide the Department with the telephone number of the device.

d. USE WHILE DRIVING

The use of a PCD while driving can adversely affect safety, cause unnecessary distractions, and present a negative image to the public. State law permits the use of a PCD by an officer while engaged in the performance of his/her official duties. However, officers operating emergency vehicles should restrict the use of these devices to matters of an urgent nature and should, where practicable, stop the vehicle at an appropriate location to use the PCD (VA Code § 46.2-818.2.b.1).