




**Maryland-National Capital Park Police
Prince George’s County Division**



DIVISION DIRECTIVE

TITLE USE OF COMPUTERS AND INFORMATION SYSTEMS			PROCEDURE NUMBER PG752.0
SECTION Administrative Procedures	DISTRIBUTION A	EFFECTIVE DATE 09/01/19	REVIEW DATE 05/01/21
REPLACES PG752.0 “Use Of Computers And Information Systems”, issued 03/18/17			
RELATED DIRECTIVES	REFERENCES CALEA 41, 82	AUTHORITY  Chief Stanley Johnson	

I. PURPOSE

This directive defines the proper use of computer and information systems, including desk top computers, laptop computers, mobile computers, PDA’s servers, electronic messaging (E-mail), data, software and internet services, owned and maintained by the M-NCPPC.

II. POLICY

The Division is committed to providing an environment that encourages the use of computers and electronic information to support the Division’s activities. It is the responsibility of each employee to ensure that this technology is used for proper business purposes and in a manner that does not compromise the confidentiality of proprietary, protected, restricted or other sensitive information.

III. SYSTEM SECURITY

- A. Each Division employee shall execute a computer and information system policy statement (Attachment “A”).
- B. All completed policy statements shall be maintained in the employee’s Division personnel file.
- C. The Division’s mission oriented systems (CAD/RMS, MDT), as well as

USE OF COMPUTERS AND INFORMATION SYSTEMS

PG752.0

the Commission's enterprise systems, will utilize a system requiring users to change passwords every 90 days.

1. An annual audit of these systems will be conducted for verification of passwords, access codes or access violations
- D. Employees shall not share any passwords or logon ID's used on any computer systems with other persons.
- E. Employees shall not post, display, or make easily available any access information including, but not limited to, passwords.
- F. Employees shall lock their computer screen (Ctrl/Alt+Del choose "Lock" or close the lid) when using an MDT that is on and logged into and the user is not physically with the computer.
- G. Systems shall only be used by the employee that is currently logged in, or signed on to it.

IV. GENERAL SYSTEM USAGE

- A. All computer systems, data, and software owned, maintained or used by the Commission is for official use only. No employee shall use or cause to be used any computer system for personal gain or benefit of any sort.
- B. No employee shall install any personal, unapproved, or unauthorized software on any system owned or used by the Commission unless approved by the Assistant Chief, Support Operations.
- C. The Division reserves the right to monitor its computer systems at its discretion in the ordinary course of business and to examine any systems at any time.

V. ELECTRONIC MESSAGING PROCEDURES

- A. The term "Electronic messages" will include E-mail, as well as any instant messages that are transmitted or received on any Divisional or Commission owned software systems and hardware.
- B. All electronic messaging correspondence is the property of the Commission.
- C. Employee electronic messages and communications are not considered private despite any such designation by sender or the recipient.
- D. Messages sent to recipients outside the Division, if sent over the Internet

USE OF COMPUTERS AND INFORMATION SYSTEMS

PG752.0

and not encrypted are not secure.

- E. The Commission reserves the right to monitor its electronic messaging, including an employee's mailbox, at its discretion in the ordinary course of business. In certain situations, the Division may be compelled to access and disclose messages sent over its electronic messaging systems.
- F. Employees shall not access another users E-mail box without authorization. When this is necessary, it should be accomplished by tools incorporated in the software application, not by sharing passwords. This provision does not preclude or prohibit the computer systems administrator(s) from accessing E-mail boxes as part of the regular monitoring of these communications.
- G. Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with the Division's and the commission's policies concerning "Equal Employment Opportunity" and "Sexual Harassment".
- H. *Broadcast-type messages sent to all Email users outside the Park Police Prince George's County Division require prior approval by an appropriate Operations Assistant Chief (Captain), or Division Chief.*
- I. Any employee who is found in violation of this policy shall be subject to disciplinary action, up to and including termination of employment.

VII. INTERNET PROCEDURES

- A. The Division's local are network (LAN) and the Commission's wide area network (WAN), including connections to the Internet, are to be used for business-related purposes. Any unauthorized use of the Internet is strictly prohibited. Unauthorized use includes, but is not limited to: connecting to, posting, or downloading pornographic material; engaging in computer- "hacking" and other related activities; attempting to disable or compromise the security of information contained on Division computers.
- B. Internet messages should be treated as non-confidential. Anything sent through the Internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way., unless messages are encrypted.
- C. Because postings placed on the Internet may display the Division's or the Commission's address, make certain before posting information on the Internet that the information reflects the standards and policies of the Division and Commission. Under no circumstances shall information of a confidential, sensitive or otherwise proprietary nature be placed on the

**USE OF COMPUTERS AND INFORMATION SYSTEMS
PG752.0**

Internet.

- D. Subscriptions to news groups and mailing lists are permitted when the subscription is for a work-related purpose. Any other subscriptions are prohibited.
- E. Information posted or viewed on the Internet may constitute published material. Therefore, reproduction of posted information or otherwise available information on the Internet may be done only by express permission from the author or copyright holder.
- F. Unless prior approval of the Assistant Chief, Support Operations has been obtained, users may not establish Internet or other external network connections that could allow unauthorized persons to gain access to the Division's computer systems or related information. These connections include the establishment of hosts with public dial-in modems, World Wide Web (www) home pages and File Transfer Protocol (FTP).
- G. All files downloaded from the Internet must be checked for possible computer viruses. Before downloading, do not forget to store the downloaded files in a temporary directory and run a virus check.
- H. Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with the Division's and the Commission's "Equal Employment Opportunity" and "Sexual Harassment" policies.

VIII. COMPUTER MANAGEMENT AND MAINTENANCE

- A. All computer hardware and software is part of the Division inventory. New equipment will be delivered to the Assistant Chief, Support Operations or their designee who will ensure it is properly located and installed.
- B. The Assistant Chief, Support Operations or their designee shall maintain a current list of all hardware by serial number, description and location within the Division.
- C. The Assistant Chief, Support Operations shall be responsible for keeping a current written policy in regards to computer systems service and support. This policy will be based on current Commission, as well as, Divisional resources, programs and contractors.
- D. Under no circumstances will any computer user make any adjustments, changes or repairs to any hardware or software components of a computer except at the instruction or with permission of the Assistant Chief, Support

USE OF COMPUTERS AND INFORMATION SYSTEMS
PG752.0

Operations.

- E. Computer users will be responsible for keeping hardware safe from destructive sources such as liquid damage (beverages) and physical damage. Storage media (thumb drives and CD's) should be stored in protective cases and secured from theft.

IX. MOBILE DATA COMPUTERS

- A. Mobile data computers and users will be subject to all preceding policies as well as following items.
- B. All officers assigned mobile-data computers (MDC's) shall always be logged onto the mobile data system (Police Mobile) while on-duty, including part-time and overtime, as long as, the hardware/system is functional.
- C. Officers shall not engage in computer transactions while operating any vehicle owned by the Commission.
- D. Officers utilizing "Notebook" style MDC's shall fold the screen in the closed position before responding to a priority call.
- E. Officers shall disable/dim or close the screen when they are out of the vehicle for more than a few minutes.
- F. Officers that are issued removable (Notebook) MDC's will ensure they are secured in the vehicle (locked in docking position) or removed from the vehicle when the vehicle is not in use.
- G. It is the responsibility of the officer receiving possible hit information (stolen, wanted records) to review it in an expeditious manner.
- H. All potential good hits must be given to the dispatcher by radio for confirmation
- I. All stop information, requests for assistance, etc. associated with a mobile computer hit must be broadcast via radio.
- J. If an automatic hit notification is broadcast by the Mobile Data System and is **not** a good hit, the officer making the initial inquiry must send an announcement message to all other MDC users in a timely manner.

X. INFORMATION TECHNOLOGY COORDINATOR

- A. The agency's Information Technology Officer has duties and responsibilities that include, but are not limited to:

USE OF COMPUTERS AND INFORMATION SYSTEMS
PG752.0

1. Setting, modifying, and terminating individual and group computer security levels, access, permissions, and distribution access levels;
2. To ensure off site server backs-ups are conducted and maintained; and
3. Acts as a liaison with the M-NCPPC's Computer Resource Center for issues dealing with the network and domain.

End of Document

**USE OF COMPUTERS AND INFORMATION SYSTEMS
PG752.0**

Attachment A

***Maryland-National Capital Park Police
Prince George's County Division***

ACKNOWLEDGEMENT OF COMPUTER AND INFORMATION SYSTEM POLICY

As an employee of the Maryland-National Capital Park Police, Prince George's County Division, I understand that the confidentiality and protection the Division's and the Commission's information is of the utmost importance. I have read and understand the Division's policy on acceptable use of its computer and information systems, including e-mail and Internet access.

If I receive a password for access to e-mail, the Internet or any other system of electronically-stored computer information, I will use it only for authorized purposes. I agree not to use a code, access a file or retrieve any stored communication other than where explicitly authorized unless there has been prior clearance by an authorized representative of the Division. I will notify the computer system administrator (s) immediately if I believe that another person may have unauthorized access to my password.

I understand that all information stored in, transmitted to or received through the Division's or the Commission's systems of printed or computer information is the property of the Division, and is to be used for job-related purposes only. I further understand that authorized representatives of the Division may monitor the use of the Division's systems of printed or computer information from time to time to ensure that such use is consistent with the Division's policies, procedures and interest. Further, I am aware that the use of a Division-provided password or code does not in any way restrict the Division's right or ability to access electronic communications.

I am aware that any violation of the Division's e-mail or Internet access policy may subject me to disciplinary action, up to and including termination of employment.

(Print Name)

(Signature)

(Date)