

GENERAL ORDER
FAIRFAX COUNTY POLICE DEPARTMENT



SUBJECT: CRIMINAL INVESTIGATIONS INVOLVING PERSONAL COMPUTERS AS EVIDENCE NUMBER: 501.7

CANCELS ORDER DATED: 10-1-10 DATE: 10-1-11

I. PURPOSE

The purpose of this policy is to facilitate the identification, investigation and prosecution of any person who uses computers, electronic devices, or digital media in the furtherance of criminal activity.

II. POLICY

It shall be the policy of the Department that during any criminal investigation, only departmental employees who are Computer Forensics Section detectives, or personnel at the direction of a Computer Forensics Section Supervisor, shall seize and forensically examine electronic devices and associated digital media that are used in the furtherance of criminal activity. Forensic examination shall only be conducted by a Computer Forensics detective, or by those members of the department who possess a department approved certification with the approval or oversight of a Computer Forensics Section supervisor.

III. DEFINITIONS

- A. Computer Forensics Detective: Any member of the Department assigned to the Criminal Investigations Bureau Computer Forensics Section specifically trained in the techniques of computer data recovery and seizure.
- B. Electronic Device: Computer system, computer peripheral, cellular device, wireless device, PDA, digital camera, portable electronic device, portable recording device, GPS device, and any other device capable of analyzing, creating, displaying, converting, receiving or transmitting electronic, magnetic, optical or other binary impulses or data.
- C. Digital Media: Hard disk, floppy disk, optical disc, removable cartridges, RAM, tapes, flash media, magneto-optical disk, and any other media which is capable of storing magnetic, optical and/or binary coding.
- D. Forensic Examination: The use of forensically sound procedures to obtain, analyze, extract or recover data residing on electronic media in a

GENERAL ORDER
FAIRFAX COUNTY POLICE DEPARTMENT



| | |
|--|---------------|
| SUBJECT: CRIMINAL INVESTIGATIONS INVOLVING PERSONAL COMPUTERS AS EVIDENCE | NUMBER: 501.7 |
|--|---------------|

| | |
|------------------------------|---------------|
| CANCELS ORDER DATED: 10-1-10 | DATE: 10-1-11 |
|------------------------------|---------------|

way that does not alter the source data, except to the minimum extent necessary to obtain the evidence.

IV. PROCEDURES

This policy shall apply only in those cases where data residing on electronic devices and digital media are being sought as evidence in an investigation. Computers seized by agency personnel as fruits of crimes, (i.e., burglary, retail theft), shall be treated in accordance with General Order 610.1, and will not normally require the services of the Computer Forensics detective.

- A. No member of the Department, except those under the direction of a Computer Forensics Section detective/supervisor, shall turn the power on, off, or disconnect the power source, access, analyze or extract data from an electronic device or associated media in any way where it is to be seized and later analyzed by a member of the Computer Forensics Section. Electronic devices and associated media can and have been found to contain destructive programs which can alter and destroy evidence. Improper handling of such devices and media, as well as accessing files and programs, may lead to the destruction of, alteration of, or inability to analyze critical evidence. This procedure shall not preclude a member of the Department from previewing an electronic device related to searches incident to arrest where there is an immediate need to access information in relation to furthering an investigation, or where there is an immediate need relating to the danger or welfare of another.
- B. When it is determined that an electronic device and/or digital media is to be seized and processed for evidence, Department personnel shall contact the supervisor of the Computer Forensics Section, who will provide direction regarding the seizure. In the Computer Forensics Section supervisor's absence, the on-call Major Crimes Division supervisor shall be contacted.
 - 1. Where possible, a thorough forensic examination of devices and media of evidentiary value shall be conducted, and the examining detective shall provide a supplement report of findings to the investigating officer/detective.

GENERAL ORDER
FAIRFAX COUNTY POLICE DEPARTMENT



SUBJECT: CRIMINAL INVESTIGATIONS INVOLVING PERSONAL COMPUTERS AS EVIDENCE NUMBER: 501.7

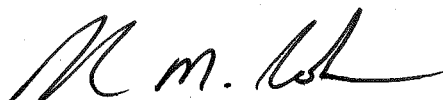
CANCELS ORDER DATED: 10-1-10 DATE: 10-1-11

2. Whenever possible, devices and media seized for evidence shall be processed in a controlled environment.
 3. When the nature of the equipment or media seized exceeds the available resources to process it, the Computer Forensics detective shall inform the case detective of that fact and assist in obtaining the required assistance.
- C. All requests for reviews, examinations and analysis of electronic equipment and media should include a copy of the Incident Report, a copy of a signed search warrant, or copy of a signed consent form before any action can be taken by a Computer Forensics detective.
- D. Training of Department personnel regarding seizure and handling of electronic devices or digital media by Department personnel shall be approved by the Computer Forensics Section supervisor prior to administration.

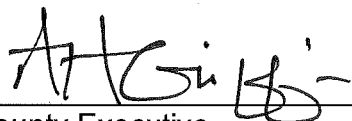
This general order becomes effective October 1, 2011, and rescinds any previous rules and regulations pertaining to the subject.

ISSUED BY:

APPROVED BY:



Chief of Police



County Executive