CITY OF CHESTERFIELD
POLICE DEPARTMENT

GENERAL ORDER 93-11

EFFECTIVE:	MAY 5, 2011	CANCELS:	GENERAL ORDER 93-02
TO:	ALL PERSONNEL	INDEX AS:	IN CAR COMPUTERS
SUBJECT:	MOBILE DATA COMMUNICATIONS		

I. POLICY

The purpose of the ***Mobile Data Communication System*** (MDCS) policy is to improve the police department's responsiveness to both public safety and criminal justice issues through the effective use of data communications in both field and investigative settings; by providing standards and guidelines for the proper and authorized use of the department's ***Mobile Data Communications System***. It is the policy of the Chesterfield Police Department that all personnel members adhere to the provisions herein regarding its ***MDCS***.

II. PURPOSE

The ***MDCS*** is designed to allow authorized members access to various federal, state and local ***Criminal Justice Information Service*** (CJIS) databases, as well as a method of non-voice communication between field units and the Communications Center.

Computerized ***CJIS*** networks include, but are not limited to; the National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), the Missouri Uniform Law Enforcement System (MULES), the Missouri Department of Revenue (DOR), the Regional Justice Information Services (REJIS), St. Louis County Police Department' Mug Shot Imaging system, Computer Aided Dispatch (CAD), Computer Assisted Report Entry (CARE), Accident Report Entry (Quickscreen), License Plate Recognition (ALPR), Mobile Ticketing System (MTS), Crime & Crime Trends (Crime Matrix) Police Department Network (PDNet), and Police Records Management Systems (RMS).

Information presented during ***MDCS*** training will also control member uses of the system and computer operation.

III. DEFINITIONS

Mobile Data Communications System (MDCS): The computers, hardware, software and other components that make up the ***MDCS***.

Mobile Data Computer (MDC): An in-car computer, a laptop or handheld, assigned to an officer or officers, individually or to a unit, as part of their assigned personal or vehicle equipment.

Member: Any employee of the police department.

Users: Members given the authority to both access and use the department's *MDCS*.

IV. AUTHORIZED USE

Members of this department SHALL NOT use the ***MDCS*** unless they have received the required training and proper authorization.

All communications and inquiries shall be for official business only. ***MDCS*** communications may be monitored, both real-time and electronically. Records of such communications may be maintained.

V. GUIDELINES

See attachment A.

VI. SAFE OPERATION

No portion of this policy is intended to prohibit or limit a user from making safety conscious decisions.

When operating a vehicle, the safe operation of the vehicle is the user's primary responsibility. Use of the ***MDCS*** is ALWAYS of secondary importance, and the user/driver SHALL ALWAYS consider the need to safely stop the vehicle before using the system if the use could divert the user's/driver's attention from the safe operation of the vehicle.

If there could be a compromise of safety, perceived or real, in any particular situation related to the use of a ***MDC***, the user is expected to use voice communications.

VII. PROACTIVE USE

The City has provided the ***MDCS*** to improve the police department's responsiveness to both public safety and criminal justice issues through the effective use of data communications and ***CJIS*** inquiries. Members are encouraged to proactively utilize the system to effectively enhance the safety and welfare of the community.

Each duty day, authorized members are required to access the ***MDCS*** to ensure they are, in an informational sense, fit-for-duty and to ensure the system is functional.

Users are required to remain connected to the ***MDCS*** throughout their tour of duty when ever possible. If system problems are encountered they are to be reported promptly.

VIII. CJIS INQUIRY PROTOCOL

The ***MDCS*** should be used as the user's primary access to the afore-referenced ***CJI Systems***, taking into consideration system availability, time, urgency, and safety.

IX. RELEASE OF LAW ENFORCEMENT INFORMATION

A. CJIS Information

Members/users SHALL NOT release ***CJIS*** information obtained via an ***MDC*** (or other method) to the public. Any requests of this nature should be referred to the Records Unit.

B. DOR Information

Members/users SHALL NOT release DOR information obtained via an ***MDC*** (or other method) that is NOT subject to public disclosure.

X. CONFIRMATION OF WANTS/WARRANTS

Records personnel should confirm any wanted person or vehicle information received via the ***MDCS***; time, safety and urgency considered. When a stop or other seizure has occurred, such confirmation shall be attempted prior to the transportation of any suspect or property for processing.

XI. MESSAGING

All communications via the ***MDCS*** will be professional and shall be conducted in a business like manner. The transmittal of any sexist, racist, vulgar, derogatory, discriminatory or provocative messages is specifically prohibited, as is the use of language that creates an intimidating, hostile, or an offensive working environment of any kind.

All messaging, even work-related, shall be limited in length and duration necessary to accomplish the task or convey the message.

XII. SYSTEM SECURITY AND MAINTENANCE

It shall be the assigned member's responsibility to ensure the security of the *MDC* against unauthorized use. Employees shall NOT give their passwords to any unauthorized person, nor will they leave their password in a discernable written form in or near their computer. (Authorized persons are defined as REJIS employees specifically assigned as system administrators and department supervisory personnel.)

It shall be the assigned user's responsibility to physically safeguard the ***MDC*** using every precaution available (i.e., locking their vehicles when left unattended).

Users shall secure their assigned ***MDC*** display so that unauthorized persons cannot view it.

Users who temporarily leave any accessible MDCS component unattended are required to either log out of the system or lock their computer from unauthorized use and viewing.

Users shall promptly notify the Commanding Officer, Division of Operational Support, or designate, whenever the ***MDCS*** is not functioning properly and/or has been damaged, stolen, lost, or whenever it is believed unauthorized access has occurred.

MDCS computers are subject to line and/or staff inspections at any time.

Users are permitted to utilize only those programs and/or applications applicable to the purpose of the ***MDCS***.

XIII. MODIFICATIONS TO EQUIPMENT

No member/user, unless specifically authorized by Chief of Police or designate, will make any modification to the ***MDCS***, the vehicle or personal ***MDC*** set-up, or to ***MDCS*** software, except for the user defined options such as screen intensity.

XIV. SUPERVISORY RESPONSIBILITY

Supervisors will review the use of the ***MDCS*** to ensure conformance to department standards including productive use.

BY ORDER OF:_____
Ray Johnson, Chief of Police Date

APPROVED BY:_____
Michael G. Herring, City Administrator Date

cc: City Attorney

CALEA REFERENCE

41.3.7

CHESTERFIELD POLICE DEPARTMENT
IN-CAR COMPUTER GUIDELINES

SILENT DISPATCHING:
DEFINITION: Silent dispatching is limited to those calls that can be dispatched with the minimum amount of radio traffic, usually limited to the car number and the nature code. All information pertinent to the call will be in the comments section of the call. Officers need only acknowledge receipt of the call.

Following is a list of calls, eligible for silent dispatch:

AANO = Auto Accident No Injuries
AAUTO = Abandoned Auto
ADM = Administrative
ALARC = Attempt Larceny (Report Only)
ASLT = Assault (Report Only)
BARK = Barking Dog
Bike = Bike Patrol
BOGUS = Bogus Check
CALL = 10-21
CARE = Care Report
COURT = Court/Prosecutor
LSART = Lost Article
MAINT = Vehicle Maintenance
NOTIFY = Notification
PCR = Public Community Relations
RADIO = Radio Repair
RCPROP = Recovered Property
CWELF = Check Welfare
DPROP = Destruction of Property (Report Only)
DUMP – Illegal Dumping (Report Only)
ESCORT = Bank Escort
FPROP = Found Property
FRAUD – Fraud (Report Only)
GO = 10-25
ILPARK = Illegally Parked Vehicle
INV = Investigation
LARC = Larceny
RETURN = Missing/Runaway Return
STAT = Station Assignment
STLIC = Stolen License
TOPHON = Threatening/Obscene Phone Call
TRUANT = Truancy
VACR = Vacation Return

If the CFS is generated in the Communications Bureau, the dispatcher will computer dispatch the officer **and** voice dispatch, "[Car#] are you clear on the [Nature Code]?"

If the Officer puts himself out on a call on one of the above, the dispatcher is not required to give a verbal acknowledgement.

OFFICER WILL NOT USE THE COMPUTER TO PUT THEM SELVES OUT ON TRAFFIC!

Use of the Mobile Net Computer: For Log Ons

Officer will start the FR Query program and then put their unit number (5C??) in the unit id, then enter their dsn into the DSN field (5???) , in the vehicle field, enter your WT emergency number followed by the letter R, in password field type "1234", then enter your REJIS login and your REJIS password and submit the information. You will get a message back indicating that you have been logged on.

Officers can either go 10-41 over the mobile net log on, over the radio, or by calling in over the telephone to the Bureau of Communications. There will be NO 10-41 information accepted over the FR Query message system.

All cars must go 10-42 over the radio or telephone.