SHERIFF OF GARFIELD COUNTY
LOU VALLARIO

107 8TH Street
Glenwood Springs, CO 81601
Phone: 970-945-0453
Fax: 970-945-6430

106 County Road 333-A
Rifle, CO 81650
Phone: 970-665-0200
Fax: 970-665-0253

GARFIELD COUNTY SHERIFF'S OFFICE
POLICY / PROCEDURE
PATROL

SUBJECT: MOBILE DATA TERMINAL USE

EFFECTIVE DATE: January 01, 2024

POLICY:
The Garfield County Sheriff's Office protects sensitive and personal information consistent with CCIC and NCIC regulations. Employees using Mobile Data Terminals (MDTs) shall comply with all appropriate Federal and State rules and regulations. MDTs are for use in patrol vehicles to provide field units with immediate access to the CCIC/NCIC system. The ability to safely access information services is an essential job requirement.

PURPOSE:
To provide Deputies guidance on the Sheriff's Office policy concerning the access, use, and security of Mobile Data Terminals.

DEFINITIONS:
- **CBI:** Colorado Bureau of Investigation
- **CCIC:** Colorado Crime Information System
- **MDT:** Mobile Data Terminal
- **NCIC:** National Crime Information System
- **OSN:** Operator Security Number

METHOD:
A. ACCESS:
   a. Access to CCIC/NCIC through MDTs is regulated by the Garfield County Sheriff's Office CCIC Coordinator. Personnel who have been granted access to this system shall abide by all rules/regulations as set forth by CBI and NCIC. It will be the responsibility of each Deputy to maintain their CCIC certification.
   b. The use of MDTs to access the CCIC/NCIC system is strictly limited to those who have completed training and been issued OSNs.

B. SECURITY:

a. MDTs installed in patrol vehicles are secured with locking mounts for security when the MDT is in use. It is the responsibility of the Deputy to ensure the security of his/her MDT when the Deputy is not on duty.
b. CCIC/NCIC security is maintained through the use of OSNs. It is the responsibility of each employee granted access to the CCIC/NCIC system to ensure that he/she is properly logged off the system when not using it.
c. It is the Deputy's responsibility to ensure the security of the MDT against unauthorized use or viewing of information. Deputies must use due care and safeguard an MDT whenever he/she is using one.
d. If a Deputy must leave the vehicle, turn down the screen brightness so that the screen is not visible from outside the vehicle.
e. Deputies will not give their password to any other person or leave their password in any discernible written form in or near his/her MDT.
f. No Deputy shall load personal programs onto his/her MDT without prior authorization.

C. USE WHILE DRIVING

a. Use of the MDT should generally be limited to times when the vehicle is stopped. When the vehicle is in motion, the Deputy should only attempt to read messages that are likely to contain information that is required for immediate enforcement, investigative, or safety needs. At no time when the vehicle is in motion should the display be viewed by the Deputy for entertainment, including Internet browsing, use of social media, or e-mail.
b. Short transmissions are permitted if it reasonably appears it can be done safely. In no case shall a Deputy attempt to send or review lengthy messages while the vehicle is in motion.

D. MISCELLANEOUS

a. MDTs shall be used to transmit official messages. MDTs shall not be used to transmit any message of a defamatory, derogatory, inflammatory, racist, or sexual nature. All transmissions are recorded and subject to audit. There will be no expectations of confidentiality or privacy.
b. Whenever reasonably possible, Deputies will not use units with malfunctioning MDTs. Whenever Deputies must drive a unit in which the MDT is not working, they shall notify Dispatch. It shall be the responsibility of Dispatch to record all information that will then be transmitted verbally by radio.
c. When investigating reports of possible bombs, Deputies shall not operate an MDT within 300 feet of a suspected device. Operating the MDT may cause some devices to detonate.