RENO POLICE DEPARTMENT GENERAL ORDER

This directive is for internal use only and does not enlarge this department's, governmental entity's and/or any of this department's employees' civil or criminal liability in any way. It is not to be construed as the creation of a particular standard of safety or care in an evidentiary sense, with respect to any complaint, demand for settlement, or any other form of grievance or litigation. Violations of this directive, if substantiated, can only form the basis for intra-departmental administrative sanctions.

Chief of Police: Jason Soto /s/		
Approving Deputy Chief: Thomas Robinson		
General Order No: E-160-04	Issued: Sept. 16, 2004	Revised: Sept 23rd, 2021
General Order Title**: ELECTRONIC COMMUNICATION**		

I. POLICY

All departmentally owned and/or issued devices are subject to entry, search, and inspection without notice as they contain information considered a public record and that are discoverable in legal proceedings or by a public records request. Employees, therefore, have no expectation of privacy when using departmentally owned and/or issued devices. Additionally, work-related information that is generated, shared, viewed and or transmitted on any device is considered a public record and may be discoverable in legal proceedings or by a public records request. As such employees are encouraged to refrain from using personally-owned devices to conduct work-related activities.

Communications that are shared on departmentally owned and/or issued devices, and work-related communications that are shared on any device, are governed by departmental policies, city policies and applicable laws.

II. DEFINITIONS

Electronic Communication Device – Devices that are used for information and communication, such as generating documents, telecommunications, text message or data transmission and which may have the ability to access the internet, E-mail, departmentally authorized software, departmental reporting systems and other applications. These include but aren't limited to computers, MDT's, mobile devices.

MDT – Mobile Data Terminal (MDT) refers to a system of radio frequency digital data transmissions via the computer terminals in police vehicles. MDT's access several criminal information databases, the computer-aided dispatch system, and records systems.

Mobile Application – software designed to run on a Mobile Device.

Mobile Device – a general term for any handheld Electronic Communications Device. It may include, but isn't limited to cellular phones, smart phones, laptops and electronic tablets.

AVLL – Automatic Vehicle Locator (AVLL) function refers to a command on the Computer Assisted Dispatch system that allows for real-time vehicle tracking of vehicles.

III. PROCEDURES

A. Employee Responsibilities – Employees that are assigned a departmentally issued Electronic Communication Device or who use a departmentally owned and/or issued Electronic Communication Device are responsible for:

1. Care and security of any departmentally owned and/or issued devices.
2. Reporting damage to and/or loss of any departmentally owned and/or issued device(s) to their supervisor and departmentally assigned IT technician as soon as possible.
3. Complying with departmental and city policy when using departmentally owned and/or issued devices.
4. Complying with departmental and city policy when engaged in work-related activity on any electronic device.
5. Protecting work-related electronic information from being viewed, accessed or shared with non-authorized personnel.
6. When operating a bicycle, motorcycle or other vehicle, exercising caution when using any device to avoid diverting attention.
7. Using AVLL as an officer safety tool for real time location of units in the field.
8. Using only those Mobile Applications that are on the department's List of Approved Mobile Applications Training Bulletin, when using departmentally owned and/or issued devices or on any device for work related purposes.

B. Prohibitions – Employees are prohibited from:

1. Installing any program, software and/or Mobile Application on a departmentally owned and/or issued Electronic Communications Device without obtaining approval from their chain of command and the departmentally assigned IT Technician.
2. Using any software, Mobile Application and/or systems that is not authorized.
3. Copying, transferring or violating any licensing agreement of any departmental and/or city systems.
4. Using departmentally owned and/or issued devices for storing personal data or for viewing, accessing or sharing personal data.
5. Accessing the internet while on-duty for non-work related purposes.
6. Sharing and/or allowing others to use their assigned username and/or password you use to login to departmental and/or city systems.
7. Using another's username and or password to access any departmentally owned and/or issued device or to access any departmental and/or city system.
8. Damaging and/or altering departmentally owned and/or issued devices.
9. Using Mobile Devices while driving unless performing work related duties.
10. Using any device in a manner that is disruptive or that interferes with productivity or compromises workplace safety.

C. Supervisors Responsibilities – In addition to adhering to the provisions listed above in sections A and B, supervisors are also responsible for:

1. Conducting random, monthly MDT audits. Each employee should be audited at least once during a shift rotation.
2. Ensuring damaged, lost or missing departmentally owned and/or issued device(s) are reported to the departmentally assigned IT Technician and Supply Technician as soon as possible.
3. Ensuring employees under their supervision are in compliance with this general order.