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: Steven Pitts /s/			
Approving Deputy Chief: Mac Venzon			
General Order No: E-160-04	Issued: September 16, 2004	Revised: May 1, 2012	Supersedes: 1/430.000
General Order Title**: ELECTRONIC DATA TRANSMISSION**			

POLICY

Electronic data transmissions are governed by Reno Police Department operating procedures, City of Reno operating procedures, government statute, and Federal Communications Commission regulations. These procedures regulate the use of electronic data transmission by Department employees via e-mail, local area networks, alphanumeric paging, facsimiles, mobile computer terminals, the Internet, cellular telephones, and remote access communications. All electronic transmissions should be conducted in accordance with NRS 281.481(7).

DEFINITIONS

LAN – The Local Area Network (LAN) is the Police Department's PC-based computer network. The LAN supports operations of alpha-paging systems, the MDT system, and electronic mail within the Department and other agencies. To facilitate communications, the LAN is networked with a series of other government agencies.

LAN Administrator – A City of Reno employee is assigned as the LAN administrator, with responsibility for managing and regulating operations of electronic data transmissions and LAN operations. The LAN administrator coordinates a data processing committee, representing Department divisions, and setting policy and determining data processing system development needs.

E-Mail – Electronic mail (E-Mail) is a messaging system supported by the LAN and Internet. E-Mail communication is available to all Department employees for work-related purposes and is linked to a variety of other City and governmental agencies.

Alphapage – Alphapage is the term used for the Department's alphanumeric paging system, which is operated from the LAN. Alphapage is an emergency notification system, and provides work-related communication among Department employees.

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 data bases, the computer-aided dispatch system, and records systems. E-Mail for work-related purposes is supported by the MDT system.

QAVL – Query Automatic Vehicle Locator (QAVL) function refers to a command on the Computer Assisted Dispatch (CAD) system that allows for real-time vehicle tracking of vehicles equipped with air cards.

Fax – Facsimile (fax) machines are provided to transmit documents electronically to individuals and other agencies for work-related purposes.

Remote Communications – Remote access consists of computer hardware and software allowing access to the LAN from remote locations via modem, ISDN, or other data-transfer protocols.

Internet – Internet refers to the worldwide computer network which facilitates e-mail, information-sharing, research, commercial activities, and program access. The Department provides employee access to the Internet for work-related purposes by approval of the Chief of Police or his designee.

Cellular Telephones – Cellular telephones use analog or digital transmission technology through public communications companies.

PROCEDURES

Electronic Data Inspection and Privacy

All Department-owned and/or operated electronic data systems, including but not necessarily limited to data, voice, and E-Mail boxes, pager memory, and electronic data storage devices are subject to entry, search, and inspection without notice. Employees, therefore, have no expectation of privacy when using Department-provided equipment and systems.

General Electronic Data Transmission Regulations

Electronic data transmission by e-mail, MDT, alphapage, fax, remote communication software, and Internet, is available for authorized employees as an alternative to typewritten or hard copy memoranda and reports, and as a messaging system for work-related purposes between employees and other agencies. Messages to individuals or groups, *e.g.,* PDEveryone, detectives, media, etc., will conform with City and Department policies, procedures, and all applicable State and Federal laws.

Messages among groups or between individuals must comply with Department operating procedures. Electronic data transmissions using City hardware and software are classified as a public record, and should not be considered a private transmission. Electronic data transmissions may potentially be discoverable in a legal proceeding and employees are accountable for complying with City and Department regulations concerning the content of transmissions.

System Management and Policy Compliance

The LAN administrator is responsible for monitoring usage of electronic data transmissions. Monitoring may include electronic recording of e-mail, fax, alphapage, MDT transmissions, and remote access sessions. Statistical analysis of transmissions allows the LAN Administrator to efficiently program system software and to maintain hardware. Recording of transmissions provides supporting documentation for case investigation, calls-for-service records, and auditing to determine policy compliance. The LAN Administrator and designated supervisors have access to electronic data transmission records for work-related purposes only.

- Supervisors and officers may use the QAVL function as an officer safety tool and real time locations of units in the field
- Random MDT audits (MSG) on patrol personnel should be conducted by the Patrol Watch Commanders on a monthly basis during a bid cycle. It is recommended that these audits, at minimum, cover an employee's ten hour shift. Each employee under the supervision of the Watch Commander should be audited at least once during a bid cycle.

Data Removal, Copying, Transferring, or Destruction

Only the LAN Administrator and those persons with formal authorization shall delete, alter, or move files maintained in common access areas of the LAN.

- The LAN Administrator may remove or delete electronic data files maintained anywhere on the LAN that are in violation of City and/or Department procedures, statute, FCC regulations, or LAN Administrator System guidelines.
- Employees should not maintain electronic data for storage purposes only. The LAN Administrator may issue storage guidelines and establish time limits for removal of data on any Department data-processing equipment.
- Employees shall not install, maintain, or operate software on the LAN or any Department data processing equipment unless authorized by the LAN Administrator. This includes game software and programs not approved for use by the LAN Administrator.
- Software licensed to the Department shall not be copied, transferred, or used in violation of software licensing agreements.

Passwords and Unauthorized Access

Employee network and e-mail passwords will not be shared nor provided to persons other than the original password-user. Employees shall send electronic data transmissions under their own password and LAN network identifier only. Accessing and/or sending e-mail messages by persons other than the authorized recipient/sender is prohibited. The LAN Administrator is authorized to access data throughout the LAN system for work-related purposes regardless of password or other access protection.

Remote Communications and Data Storage

The Department maintains a system of remote communications allowing employees access to the LAN via modem, ISDN connection, or other data transfer protocol for work-related purposes. Remote access is provided at police substations and is also authorized for connection to

personal computer equipment and home residences of approved employees. Employees are responsible for protecting information and access to the LAN via remote communications.

- Employees will not allow non-Department personnel access to Department remote communications, nor allow tampering with or copying of Department software.
- Employees are responsible for insuring data transmissions via remote access and data storage media utilized on Department computers is free of any software virus or information that violates departmental regulations.
- Employees are responsible for assuring the protection and control of work-related information stored on data storage devices, *i.e*., floppy disks, hard drives, and laptop computers, against any unauthorized release.

Internet

The Department may provide employee access to the Internet for work-related purposes. Since the Internet is a decentralized communications network with little formal regulation, the potential for computer virus infections, unauthorized access to the LAN by users outside of the Department, and Internet activity that violates criminal and civil law, is high. Employees accessing the Internet via Department electronic data transmission systems must comply with the following:

- They must follow LAN Administrator guidelines for access and data transmission.
- Transmissions sent to Internet users and groups via Department data transmission equipment must comply with City and department policies, procedures, regulations, and City ordinances, as well as State and Federal laws.
- Employees will not access Internet addresses, World Wide Websites, or transfer files, unless required to as a function of their job assignment. This includes accessing information of a sexual nature, for entertainment purposes, or for commercial gain by the employee.
- The LAN Administrator may monitor Internet activity by employees and may restrict access to Internet information.
- Employees will not encrypt or transmit or receive encrypted data, unless the LAN Administrator is provided with a key, password, or other decryption enabling monitoring of data.

Cellular Telephones

Cellular telephones are provided to certain employees and for specific assignments for work-related purposes. The following guidelines will be followed while in possession of departmental cellular telephones:

- City of Reno cellular telephone numbers will not be broadcast on City mobile radio channels.
- Cellular telephone numbers will not normally be given to citizens. Upon receiving or making a call, the user should advise the caller that they are using a cellular phone and ask not to be placed on hold.
- Employees should make every effort to minimize cellular telephone expenses by using landline telephones whenever possible.
- Long distance calls should only be placed in the event of an emergency.

- Employees operating a motor vehicle should use caution when using a cellular phone to avoid diverting attention from safe driving.
- The phone user is responsible for securing vehicles and/or securing their cellular telephone to prevent it from being stolen.