Effective communication systems are essential to law enforcement. Communications systems are only as effective as the people who operate them are. For this reason it is essential that all employees comply with established SnoPac Radio Procedures Manual.

## 8.10 MOBILE DATA COMPUTERS (MDC)

Employees of the Everett Police Department who have access to Mobile Data Computers or other department computers that have access to CAD/RMS will comply with all policies and procedures governing the proper use of that equipment as described in the Everett Police Department Policy and Procedure Manual, the SNOPAC Radio Procedure manual, and the City of Everett Electronic Communication and Network policies.

Any introduction of unauthorized software programs or other files are strictly prohibited.

Employees are prohibited from the manipulation or alteration of current software running on agency owned mobile, desktop or handheld computers.

The use of CAD/RMS for personal reasons is prohibited.

## 8.11 COMPUTERS

Any unauthorized entry into files or computer programs by employees ~~are~~ is grounds for immediate disciplinary action. All employees must comply with the city policy on computer use.

The introduction of outside disks or software into agency owned computers is generally prohibited. Such an introduction could result in a virus infection and as such, any outside software must be inspected and approved by Computer Services, prior to installation. All employees will be trained on and comply with the City of Everett Electronic Communications and Networks Policy.

The ACCESS computer system is the property of the Washington State Patrol. The system allows inquiries against numerous state and federal computerized databases. Additionally, the system provides a means of transmitting point to point Teletype messages to other law enforcement agencies both in and out of state. Operation of the system is to be conducted under the rules of the ACCESS, WACIC and NCIC procedure manuals. Violations of those rules may result in agency disciplinary measures and/or criminal prosecution if criminal conduct is identified. Disciplinary measures imposed by the WSP may include revocation of individual certification, discontinuance of system access to the department, or purging the department's records.

## 8.12 BROADCAST CODES

Policy and procedures for dispatch and clearance codes are in the SnoPac Radio Procedures Manual. The Administrative Services Division assigns department radio call numbers.

Updated &
uploaded
3/25/11

## 8.11 COMPUTERS

Any unauthorized entry into files or computer programs by any employee~~s~~ ~~are~~is grounds for immediate disciplinary action. ~~All employees must comply with the city policy on computer use.~~

The introduction of outside disks or software into agency owned computers is generally prohibited. Such an introduction could result in a virus infection and as such, any outside software must be inspected and approved by ~~Computer Services~~Information Technology, prior to installation. All employees will be trained on and comply with the City of Everett Electronic Communications and Networks Policy.

**Formatted:** Normal, Tab stops: 0.3", Left + 0.7", Left + 1.1", Left + 1.5", Left + 1.9", Left + 3.9", Left + 5", Left + 5.25", Left

The ACCESS computer system is a computer controlled communications system operated and maintained by the ~~property of the~~ Washington State Patrol. The system is operable on all department computers that have the capability to conduct inquiries (Department of Licensing, NCIC, WACIC, etc) and ~~The system~~ allows inquiries against numerous state and federal computerized databases. Additionally, the system provides a means of transmitting point to point Teletype messages to other law enforcement agencies both in and out of state. Operation of the system is to be conducted under the rules of the ACCESS, WACIC and NCIC procedure manuals. The ACCESS system shall only be used for official law enforcement business.

The Records Manager is designated as the ACCESS Terminal Agency Coordinator (TAC) to act as the point of contact for the WSP and the FBI. This individual ~~will be~~is responsible ~~to~~for ensureing compliance with state and NCIC policies and regulations. Responsibility for proper operator performance, strict adherence to regulations, prompt notification of CJIS violations to the ACCESS Section, and subsequent training rests with the TAC. The TAC also makes sure that all terminal users, including mobile data terminal users, maintain ACCESS certification every two years.

Each user must observe all restrictions placed on the use or dissemination of information received through ACCESS. Information obtained through ACCESS must only be used for criminal justice purposes. Users shall not use any information obtained through the ACCESS system, including DOL and DOC information, for private business or personal reasons or furnish any information so obtained to any other person for such use.

Maintaining security of the terminal sites and information received is the responsibility of agency personnel operating the terminal, the TAC, and the agency head. Terminal locations must be secure from unauthorized access, and all employees authorized to use the system shall be instructed on the proper use of equipment and the dissemination of information received. Federal and state laws protect the information provided by ACCESS.

Violations of ~~those~~these rules may result in agency disciplinary measures and/or criminal prosecution if criminal conduct is identified. Disciplinary measures imposed by the WSP may include revocation of individual certification, discontinuance of system access to the department, or purging the department's records.

updated c̄ uploaded 9/8/11 KAD