SUBJECT: Computer Software and Radio Equipment		
2.6	**EFFECTIVE:** 9-7-2022	*Bryan Wheeles* Bryan Wheeles, Chief of Police
	REVISED: 8-24-2022	
	TOTAL PAGES: 11	

2.6.1 PURPOSE

To provide guidelines for the use of computer and radio equipment by Department members.

2.6.2 POLICY

Computers, communication equipment and radios shall be used for law enforcement purposes except for limited uses outlined by policies. Department employees shall comply with all City, Department and Federal, Local and State laws concerning use of computers, communication equipment and radios.

2.6.3 COMPUTERS AND COMMUNICATIONS EQUIPMENT

A. In General

1. Use of all City communication systems should be limited to City related activities. However, in all cases the Department shall strictly adhere to the City of Topeka Acceptable Use of Technology Systems, which does not prohibit the personal use of City communications systems, within reason.
2. Communication system contents are not protected or privileged and may be subject to disclosure under the Kansas Open Records Act or discovery during civil/criminal litigation, including stored or deleted data on the system. This extends to storage of confidential information on computers and all necessary precautions taken for security.
3. Classified, confidential, sensitive, proprietary or private information/data must not be disseminated to unauthorized persons or organizations by hard copy, electronic transmission or by viewing on computer screens.
4. Management may, without notice, access data, text caches, pager memory banks, e-mail, voice mail and other employer provided electronic storage systems for administrative purposes. This may include deciphering of encrypted text.

5. Ordinarily, employees should not access communications intended solely for another employee unless requested to do so by the intended recipient, or lawfully directed to do so by a superior.
6. No employee shall incur costs to the Department for personal use of information technology or related services.
7. No employee shall store or display inappropriate material on Department premises or equipment, unless needed for investigative purposes and authorized by the Bureau Commander. All computers will be logged off at the end of each workday; and when away from the work area for extended periods or off duty.
8. Only authorized personnel may connect, disconnect, reconnect, reconfigure or enter the CPU.
9. Officers shall not intentionally disable Global Positioning Satellite (GPS) tracking software or device(s) on any issued equipment without supervisor's approval.

B. Hardware and Software

1. External hardware and/or corresponding software shall not be used on LEC computers without permission from an individual's Bureau Commander and Information Technology (IT).
2. Department owned software and related documentation shall not be copied.
3. Personally owned or new software may only be used with prior authorization from the Bureau Commander and IT before installation.
4. Executable files or programs shall not be downloaded without prior approval from IT.
5. Social media sites shall not be used, unless needed for investigative purposes or authorized department information that is released on social media.
6. Email

    a. Department employees use the email system both formally and informally. Formal emails are those that either contain or have an attachment that serve a written directive function (clarify policy, personnel announcements, legal bulletins, administrative instructions, etc.) and/or contain a supervisory directive. These emails shall be treated the same as if they were a formal Department special order, policy clarification, administrative memo, or other formal informative memo in hardcopy.
    b. Formal emails carry the same responsibility for review and procedural regulation as a formal memo would.
    c. Employees shall be considered notified of any Department correspondence when the correspondence has been sent to their Department email account.

d. Employees shall be required to check the Department email accounts at least once per scheduled workday. Employees shall be responsible for reading and responding to any formal Department correspondence distributed via the email system.
e. The email system "read" receipt function may be used to document the transmission and receipt of an email message. It is not required but may be used discretionally for message tracking purposes.
f. Email system failures, equipment malfunctions, travel status, or other circumstances that prevent ready access to the email system, shall be considered in the event an employee is alleged to have violated section "d" above.

C. Information Technology Staff

1. IT shall perform a systems backup daily, Monday through Friday, and hold it for at least 2 weeks.
2. IT shall authorize all software installed in the Department and ensure software copyright laws are observed.

D. Records Passwords and Access Codes

1. Passwords and access codes shall be maintained on the central records computer system. Passwords shall be changed every 90 days.
2. An annual audit will be performed of the central records computer system for verification of all passwords, access codes, or access violations.

E. Laptop Computers

1. Employees using a laptop computer outside of the LEC shall use any and all security features associated with the laptop.
2. Employees are responsible for the care of the laptop and associated equipment.
3. Employees will not leave the laptop in areas subject to extreme heat and/or cold or in direct sunlight.
4. Employees will not leave the laptop unattended for extended periods of time in places where theft is a possibility.

F. Wireless Telecommunications

1. Cellular phones may be issued to Department staff approved by the Chief of Police whose response to emergencies or urgent calls requires unrestricted voice communications with a wide range of persons and offices.

2. Employees shall use great caution when driving while using a cellular phone.
3. Employees must be aware that persons can monitor cell phone conversations with scanners and conduct themselves accordingly.
4. Excessive personal use of Department cell phones is not acceptable and may lead to forfeiture of the cell phone.
5. Each Bureau is responsible for the cell phones in use in their Bureau. Supervisors shall reference City Policy for other regulations on cell phone use.
7. Employees shall follow the City's Policy on cellular phone use.

2.6.4 MOBILE DATA TERMINAL

A. System Operation

1. The MDT shall be turned on and logged into the system at the beginning of each officer's shift. The MDT will remain on at all times that the officer is on duty.
2. The MDT should not be used while the vehicle is in motion. The officer must focus attention on safe vehicle operation.
3. Computer Aided Dispatch (CAD)

    a. The MDT shall be used in conjunction with radio communications and is not intended to be a replacement for voice dispatching.
    b. The MDT may be used to reduce radio communications, enhance officer safety and provide a means of transmitting information and messages.
    c. SCECC personnel shall continue to dispatch calls for service over the radio.

        1) Initial dispatches may be brief with additional information sent via the MDT.
        2) If a call is extremely sensitive due to security, hazards, or other circumstances, SCECC personnel may choose to dispatch only using the MDT. In this situation, SCECC personnel will announce, via the radio, that a call is being dispatched via MDT only.

4. MDT's should generally be used by both officers and SCECC personnel to communicate non-urgent information that would otherwise tie up radio time. If an officer chooses to use the radio instead of the MDT, SCECC personnel shall respond to the officer on the radio.

B. Criminal History Records Database

1. Information contained in Criminal History Records Information (CHRI) systems is not public information and shall be accessed for law enforcement purposes only and in conformance with Department policy, NCIC Records Entry, and Information Dissemination.
2. Warrant information received through these databases shall not be considered probable cause for arrest until properly verified and confirmed with the originating agency by SCEEC.
3. Officers may only use the CHRI databases after they have been properly trained and certified. Officers will only use the databases in accordance with Department policies.
4. Officers should use their MDT to conduct routine vehicle and/or person checks in order to relieve SCECC workload and reduce radio traffic.

C. MDT Messaging Function

1. The MDT messaging function may be used to communicate with any other unit on the system.
2. Officers shall not send KCJIS and CJIS sensitive data via email.
3. All messages are recorded and may be considered public information. The following guidelines, along with City of Topeka Policy regarding the use of Information Technology Systems, shall be observed when using the messaging function:

    a. Messaging should only be used for police related matters, consistent with the City's Telecommunications Policy; and
    b. Remarks containing degrading or unprofessional comments shall be prohibited.

D. MDT Security

1. Information displayed on the MDT screen in the active window is confidential and caution should be exercised to ensure unauthorized personnel do not view it.
2. Vehicles equipped with MDTs shall be locked when not in operation or occupied by an authorized user.

2.6.5 NCIC RECORDS ENTRY, RESPONSE AND INFORMATION DISSEMINATION

A. NCIC Records Entry and Response

1. NCIC Entry Requests

a. Records/SCECC shall be responsible for entering or modifying entries on wanted and missing persons, stolen motor vehicles, boats, stolen tags and all stolen property. Requests will be made on an Offense Report, Supplemental Property Report or Wanted/Missing Person Report.
b. Officers will gather the necessary information and contact SCECC as quickly as possible with the necessary information for a bulletin and entry into NCIC. The report(s) will be forwarded to the Records Unit.

2. NCIC Entry Modifications: Additional or corrected information on an NCIC entry will be forwarded as quickly as possible to the Data/Records Unit as stated above.
3. NCIC Inquiries: At the time of inquiry, officers will advise if the person or article is in their presence. These inquiries will have priority over inquiries on persons or articles not in an officer's presence.
4. Positive Response to Inquiries (HIT)

    a. An NCIC HIT provides cause to detain persons for a reasonable amount of time to confirm information. An officer must receive confirmation prior to making an arrest, clearing the missing status of a person or seizing stolen property. The officer and dispatcher shall take reasonable steps to ensure:

        1) The person or property under inquiry is the same as listed on the HIT;
        2) The warrant, wanted/missing person or theft report is still active; and
        3) Correct information is relayed to the officer on extradition or the return of missing persons or stolen property.

    b. When the dispatcher confirms a HIT, the officer's decision to take action must be based on available information known at that time.
    c. SCEEC shall be notified as soon as possible after the arrest of the person or seizure of the property so the appropriate location and/or cancellation procedure information can be initiated.

5. Removal of NCIC entry: Any officer who discovers a person or article entered in NCIC is no longer being sought will notify SCECC or Records Unit as soon as possible to initiate cancellation procedures and complete appropriate reports related to the incident.

B. NCIC Records Validation

1. All NCIC records must be validated to confirm the record is complete, accurate, and still outstanding or active.
2. A case file must be maintained with documentation for information entered into each field of an NCIC entry. This information is maintained for future review/validation. This file will also contain the most current validation record or worksheet.
3. Validation is achieved by doing the following:

    a. Retrieve and review the original entry (case file) and current supporting documentation.
    b. Consulting with any of the following: complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual.

        1) Write a letter to the victim, etc. with a description of the item or person in NCIC.
        2) Upon return of a letter indicating the item/person is still missing, complete a worksheet indicating what action is to be taken. If a letter is NOT returned, complete as in Section B.5 below.
        3) Retain the letter and worksheet if the item/person is to be retained in NCIC.
        4) If the item/person is cancelled from NCIC, the cancellation and worksheet are put in the case file.
        5) If the case file is in media storage and the item/person is canceled from NCIC, shred the information.

    c. Review whether any additional information has become available since the original entry that could be added.
    d. Warrants will be verified as to whether they are still outstanding and whether extradition is still authorized.
    e. Contact the reporting party of a missing person to verify they are still missing.

4. The NCIC worksheet is not sufficient for validating an NCIC entry.
5. If attempts at validation are unsuccessful, make a determination based on the best information available whether or not to retain the original entry.

C. Dissemination of Criminal History Information

1. All employees shall ensure the contents of released information are limited to:

    a. Guidelines as set by law and NCIC regulations;

b. Criminal justice agencies for purposes of the administration of criminal justice or law enforcement related agency employment;
c. Individuals and agencies which require criminal history record information to implement a statute or executive order expressly referring to criminal conduct and contains requirements and/or exclusions expressly based upon such conduct;
d. Agencies of State or Federal government which are authorized by statute or executive order to conduct investigations to determine employment suitability or eligibility for security clearances allowing access to classified information;
e. Individuals and agencies where authorized by statute, regulation, court order or court ruling;
f. Use of criminal history record information disseminated to non-criminal justice agencies under these regulations shall be limited to the purposes for which it was given and may not be disseminated further; and
g. No agency or individual shall confirm the existence or non-existence of criminal history record information for employment or licensing checks except as provided in current Department of Justice rules and regulations.

2. Audits

a. The Department is subject to audits conducted by the State and/or the FBI to verify adherence to these regulations. Employees shall generate and maintain appropriate records to facilitate such audits.
b. Such records shall include, but are not limited to, the names of all persons or agencies to whom information is disseminated and the date upon which such information is disseminated.

3. Penalties

Any agency or individual violating these regulations shall be subject to disciplinary action up to and including termination of employment, in addition to possible criminal and civil penalties.

4. Security Violations

a. All NCIC security violations shall be immediately reported.
b. All ex-employees and employees under disciplinary leave must be removed from CJIS system access immediately.

2.6.6 RADIO EQUIPMENT

A. Program Objectives

1. Each full time officer is provided with a hand-held radio, case, charger and speaker microphone to:

    a. Establish an efficient communications network to handle calls for service;
    b. Provide an immediate communications link in emergency situations;
    c. Allow officers emergency radio communication access during off-duty status;
    d. Decrease response time;
    e. Increase officer and public safety; and
    f. Communicate with other agencies.

2. No officer, regardless of rank, shall issue any hand held radios assigned to TPD to any other agency without approval of the Chief of Police.

B. Operating Procedures

1. Officers shall monitor radio traffic and respond to all dispatches.
2. The following procedure shall be followed if an officer who is required to be in radio contact with SCECC fails to respond to a radio call:

    a. If SCECC receives no response from the officer, the officer's supervisor shall be notified of the failure to respond.
    b. The supervisor shall initiate procedures to locate the missing officer and notify the Field Commander.
    c. The supervisor shall obtain an explanation from the missing officer when he or she is located and report it to the Field Commander.
    d. The supervisor shall initiate corrective action if appropriate.

C. Radio Maintenance

1. Employees shall maintain their assigned radio according to the manufacturer's recommendations. Prior to each shift, employees shall:

    a. Determine whether their assigned radio equipment is working satisfactorily;
    b. Bring any problems to their immediate supervisor as soon as possible; and
    c. Contact SCECC radio repair if service is needed or contact the TPD Quartermaster if a loaner radio is needed.

D. Uniformed officers shall carry their portable radio in a Department issued carrying case to secure the radio from falling and that is firmly secured to their duty belt.

   1. Officers desiring to use other than the Department issued case or antenna must first obtain approval from the Bureau Commander.
   2. Investigative personnel may use a belt clip radio holder.

E. Employees shall provide a secure storage location for the radio and accessories and store their assigned radios out of public view, preferably in a locked location while off duty and away from home.
F. Employees shall not leave the radio in personal vehicles for extended periods of time.
G. Lost or stolen radio: If an employee's assigned radio is lost, stolen or damaged, the employee shall immediately:

   1. Notify SCECC and the Field Commander;
   2. Complete an offense/supplement report and memo explaining the circumstances and forward them through the chain of command; and
   3. Obtain a replacement radio from the Quartermaster.

H. Officer Radio Use on Secondary Employment

   1. Officers may carry their assigned radios.
   2. Off duty officers are not required to monitor or use these radios during off duty status.
   3. Officers working extra duty who choose to monitor the police radio will keep transmissions to a minimum.
   4. Officers will not be compensated for off duty use of the police radio unless it arises out of police action needing to be taken.
   5. If the officer uses the radio while off duty and is not assigned a personal unit number, the officer shall use his or her badge number preceded by "1" (e.g., badge number 101 would be identified as Unit 1101).

I. Turning In Radios

   The Quartermaster manages the distribution and tracking of all portable radios. Officers that wish to transfer, trade, or replace radios will do so through the Quartermaster.

J. Quartermaster Responsibility

   1. The Quartermaster shall handle all hand held radio transactions.

2. No officer of any rank shall sign out and possess more than one hand held radio, charger, speaker microphone or battery without prior approval from the Chief of Police.
3. The Quartermaster shall maintain an accurate record of Department hand held radios in conjunction with SCECC database records.
4. The Quartermaster shall report any loss of radios to the Chief of Staff.
5. Issuing Radios: The Quartermaster shall communicate with Shawnee County Radio Repair regarding issuing radios.
6. The Quartermaster must process all radio transfers, trades, etc. of any kind by any Bureau.
7. The Quartermaster shall have custody of all unassigned radios.