ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE
1625.6, USE OF ELECTRONIC COMMUNICATIONS SYSTEMS

EFFECTIVE:	9/23/2013
RESCINDS:	1625.5
DISTRIBUTION:	ALL EMPLOYEES
REVIEW RESPONSIBILITY:	SUPPORT SERVICES MANAGER
ACCREDITATION CHAPTERS:	26
CHIEF OF POLICE:	ORLANDO ROLÓN

CONTENTS:

POLICY:

It is the policy of the Orlando Police Department to place proper controls over the use of electronic communications systems to ensure the lawful use of the system or equipment for effective law enforcement.

This policy establishes guidelines for the operational use, issuance, and training of electronic communications systems and equipment.

PROCEDURES:

1. GENERAL

1.1 COMMUNICATION SYSTEMS

Various "communications systems" may be utilized by, or provided to, Department employees. The systems include both real-time and pre-recorded communications. Some of these are:

a. Desk or personal computers, Internet, Intranet, and electronic mail (email).
b. AS400 computer terminals.
c. Telephones, cellular telephones, voice mail, pagers, and facsimile (fax) devices.
d. Video cameras/recorders.
e. Digital/tape recorders and players.

Employees will adhere to the current issue of P&P 1122, Police Radio Communications, when using police radios, and P&P 1902, Forensic Photography, Digital Cameras, and Digital Imaging Archive, when using police digital cameras.

1.2 PRIVACY

Employees will not access communications including, but not limited to, computer and voice/phone mail, intended solely for another employee or person unless requested to do so by the intended recipient, or directed to do so by a manager, or unless the access is done in compliance with Section 1.5 of this policy. Employees are reminded that public records or evidentiary law may require preservation and/or release of certain information.

1.3 SECRECY

Classified, confidential, sensitive, proprietary, or private information or data must not be disseminated to unauthorized persons or organizations.

Covert electronic audio interception and/or recordings will only be done as part of criminal investigations. Prior to initiating such action, employees must ensure they are acting within current court rulings. Up-to-date information may be obtained through OPD Training Bulletins. Employees are encouraged to contact the Police Legal Advisor if they are unsure of specific legal issues. Employees are reminded that public records or evidentiary law may require preservation and/or release of certain information.

1.4 PROHIBITIONS

All Departmental communications systems are intended for OPD business purposes only. Incidental and occasional personal use of Department communications systems is permitted. Such personal use may not create any additional cost to the City and is subject to such guidelines and standards as are adopted by the employee's supervisor.

Communications systems must never be used to threaten or intimidate another person. Except when incidental to an investigation or as part of an official inquiry/response or report, it is prohibited to use a department communications system to:

a. Send or knowingly play or display images that contain obscenity, nudity, or words of a prurient or sexually suggestive nature even if the recipient has consented to or requested such material.

b. Send or knowingly play or display jokes or comments that tend to disparage a person or group because of race, sex, ethnic background, national origin, religion, sexual orientation, age, verbal accent, source of income, physical appearance or agility, mental or physical disability, occupation or political beliefs.

c. Conduct personal business on/with any City computer or other equipment. This is not intended to preclude the use of available City computers for educational purposes or learning and practicing computer skills when off duty.

d. Compromise the integrity of the Orlando Police Department, the City of Orlando, or their business in any way.

Employees will not download software to City computers or load any non-approved software onto City computers unless approval has been obtained from both:

a. The Technology Management Division (TMD), AND
b. The commander having authority over said computer.

Employees will not change nor adjust settings or functions on common area equipment, or equipment normally assigned to or used by another employee.

Employees will not attach personal equipment or equipment peripherals to City electronic equipment without a commander's and TMD's approval.

Other than portable equipment (i.e., laptop computers), employees will NOT unplug, disconnect, nor move computer equipment or peripherals without written approval from their bureau commander and being coordinated through the OPD Technology Business Analyst (TBA).

The use of another's credentials (User ID and password) for computer or software application access without proper authority is strictly prohibited.

1.5 PRIVACY ADVISORY

Employees DO NOT have a reasonable expectation of privacy when using a computer or communications system that is employer-authorized or is provided for a mutual benefit. The Department retains the right to monitor employees' telephone and electronic messages, and to inspect mail or documents sent to or by employees, including the deciphering of encrypted text and the removal or inspection of any software installed on employer-provided computers.

Unless the other party does not speak or read the language, all communications shall be in English, and no encryption program shall be used without management approval.

Management representatives also may access, without notice, data or text caches, pager memory banks, email and voicemail boxes or accounts, and other employer-provided electronic storage systems except as prohibited by law. Management does not need to obtain prior judicial approval and an employee's continued employment shall act as a waiver of any claims an employee may have for infringement of privacy.

2. SUPPORT

2.1 TECHNOLOGY BUSINESS ANALYST

Normally, the Orlando Police Department's technical equipment, applications and support originates through the City's Technology Management Division (TMD). To facilitate more efficient support of technical needs, two Technology Business Analysts (TBAs) have been assigned to support OPD. The TBAs act as a liaison between OPD and TMD to coordinate projects and resources. The TBAs will be the first point of contact for the user or department in matters of technology planning initiatives, projects, training or problems. Requests for computer upgrades, additional equipment, or additional computer program installations must be coordinated through the OPD TBA.

2.2 HELP DESK

The Help Desk is managed by the City's TMD at City Hall. Help Desk personnel respond to issues concerning the AS400, personal computers (PC), mobile computers, printers, the computer network and telephone or cellular services and equipment. The Help Desk's purpose is to:

a. Receive reports of trouble with a specific computer and related equipment, such as printers, modems, etc.
b. Receive reports of trouble with the computer network.
c. Receive reports of cell phone, telephone and/or voicemail trouble.
d. Receive reports of trouble with City-supported computer programs.
e. Assist computer users with "how to" questions about City-supported computer programs.

2.2.1 SUPPORT DURING NORMAL BUSINESS HOURS

The Help Desk is staffed from 0700 to 1900 hours, Monday through Friday, and can be reached by calling 407.246.2600.

OPD Employees are required to call the Help Desk when they experience computer, printer or telephone problems between 0700 and 1800 hours, Monday through Friday. Employees will explain the problem to the Help Desk. If Help Desk personnel are unable to immediately resolve the problem, they will route the help call to the appropriate resource for response and resolution. If the OPD employee is in a field position, they shall leave their mobile computer in the Quartermaster Unit if it needs to be deadlined, along with a completed mobile computer repair form (Attachment A - also known as a "Deadline Card").

2.2.2 AFTER HOURS SUPPORT

TM provides limited support after hours. To report a problem after hours (1900 to 0700 hours, Monday through Friday; weekends; and City holidays), please refer to the TM Support Procedures, available on OPD Online, Training References page, for more details. This document also defines the procedure for escalating after-hours calls or reporting problems and requesting inmmediate on-site or escalated support for essential services (e.g., TM-supported CAD, ICJIS, Teletype, etc.).

2.3 TM CELL PHONE ADMINISTRATOR

The TMD employee designated as the TM Cell Phone Administrator shall be responsible for the service and technical support of all OPD cellular telephones and any contractual or billing issue with the service provider. If an OPD user with an assigned cellular telephone requires technical assistance (i.e., cell phone quits working or is lost) they shall contact the Help Desk by calling 407.246.2600. If Help Desk personnel are unable to address the problem, they will record a help call and forward it to the TM Cell Phone Administrator for resolution.

2.4 TRAINING

The City's TMD conducts initial training upon deployment of City-supported computer applications. After that time, it is the responsibility of the unit overseeing the software application to provide any additional or remedial training.

The City's Human Resources Division sponsors ongoing training for City-supported computer programs, such as word processing, spreadsheets, and presentation software. Additional information, including the training calendar and registration process, may be found on the City intranet, Employees tab, under the Training category.

Additional courses may be found, at very reasonable costs, through outside organizations. Information about enrollment in these courses must be processed through the OPD In-Service Training Unit.

3. COMPUTER HARDWARE AND SOFTWARE

3.1 DEFINITIONS

3.1.1 CREDENTIALS

The term "credentials" refers to the user ID and password for any computer/software application. Credentials are confidential and should be not shared with anyone.

3.1.2 MOBILE COMPUTER

The term "Mobile Computer" shall include any laptop or tablet computer with wireless connectivity.

3.1.3 MOBILE COMPUTER TERMINAL

The term "Mobile Computer Terminal (MCT)" refers specifically to ruggedized mobile computers utilized primarily in patrol or other specialty vehicles.

3.1.4 MOBILE COMPUTER COORDINATOR

The OPD Property Supervisor shall serve as the Mobile Computer Coordinator, providing inventory support for all OPD mobile computers.

3.1.5 TM UPDATER

This is software developed and utilized by the TMD to remotely send updates to OPD computers.

3.2 COMPUTER ACCESS/SECURITY

3.2.1 AUTHENTICATION

All OPD computers use dual authentication (two logins) to confirm authorized access to police data. This is in compliance with the FBI's Criminal Justice Information Systems (CJIS) requirements for advanced authentication. This procedure safeguards against unauthorized attempts to access, alter, remove, disclose or destroy stored information. Each user will use his or her individual Windows credentials and secondary login credentials to sign on or authenticate to the OPD computer network.

3.2.2 USER ACCOUNT SECURITY

Users should lock their computer when leaving it on and unattended.

3.2.3 ANNUAL AUDIT

An annual audit to verify that only authorized personnel have OPD computer access will be conducted. The results will be submitted to the Chief of Police with all discrepancies noted.

3.2.4 VIRUS CONTROL MEASURES

All computer hardware and software utilized by the Orlando Police Department will be protected with a valid antivirus software administered and maintained by the TMD. The antivirus software is updated on a regular basis by the TMD to offer the best and most up-to-date virus protection.

3.3 COMPUTER FILES MAINTENANCE, BACKUP AND RETENTION

The TMD will ensure that the Police AS400 applications and data, including but not limited to the Computer Aided Dispatch (CAD) system and the Records Management System (RMS), are replicated to the Police backup server. In the event that the AS400 fails to operate, TMD personnel will switch production from the AS400 to the police backup server. In addition to data replication, TMD will perform full backups of the Police AS400 semi-annually and will store these backup tapes at a secure off-site location until the next backup. Incremental backups are performed on a weekly basis with a 26-week retention period.

Other networked OPD computer servers including, but not limited to, OPD2 (commonly known as the N:\ drive), OPDPOL, OPDWEB1, and AEGIS2 are fully backed up to an internal backup server on a nightly basis. The encrypted full backups are kept for 45 days.

3.4 COMPUTER UPDATES

City authorized computer updates will be remotely distributed as needed. Updates initiate upon computer start-up or login. Users should reboot their computers at least weekly to ensure updates are properly deployed to their assigned desktop or mobile computer. Updates may include software updates or updates to forms and templates.

3.5 OPD INTERNET AND INTRANET WEBSITES

The Orlando Police Department maintains a web presence for both external and internal customers. An Internet Manager and an Intranet Webmaster, both appointed by the Chief of Police, shall be responsible for the development and maintenance of their respective websites.

3.5.1 OPD INTERNET

The Orlando Police Department currently maintains an internet presence for external customers through the City of Orlando's website, CityofOrlando.net. The OPD Sworn Internet Manager is responsible for posting new or updated web pages. The external site is maintained and coordinated in conjunction with the City of Orlando Office of Communications and Neighborhood Enhancement Department.

The OPD internet site may be used to provide information to the public of a general nature, or as a work tool for purposes such as recruiting, providing forms, etc. Units, sections, divisions, or bureaus may submit material to be posted on the OPD internet website. Division commanders shall ensure that their respective division's website is updated annually.

For additional information on the internet site, including submitting information for posting, please refer to the current version of P&P 1632.0, Orlando Police Website.

3.5.2 OPD INTRANET (OPD ONLINE)

The Intranet Webmaster is responsible for the development and maintenance of the internal intranet site, OPD Online. OPD Online shall be the Department's main point-of-reference for departmental communication, access to various software applications, training materials and links to other sites required for completion of law enforcement duties.

OPD Online resides on a secure server, accessible only to OPD personnel and select TM support personnel. Information to be posted onto OPD Online shall be forwarded via the chain of command to the OPD Intranet Webmaster for consideration.

3.6 INTERNET AND INTRANET ACCESS

Internet and intranet access will be granted to all employees with computer technology capable of executing the programs unless specifically denied by their bureau commander or the Chief of Police.

Incidental and occasional personal use of the internet is permitted by the City, but will be treated the same as any other use. Such personal use may not create any additional cost to the City and is subject to such guidelines and standards as are adopted by the employee's supervisor Supervisors should monitor the frequency and appropriateness of internet and social media usage in accordance with the current version of P&P 1635, Social Media, and City of Orlando policy.

Any use of the internet or intranet for "moonlighting," job searches, soliciting or proselytizing for commercial ventures, religious or personal causes or outside organizations, or for other similar non-job related solicitations is strictly prohibited, unless necessary to serve a legitimate City purpose. Abilities to download and conduct file transfers (FTP) must be authorized by the TMD. This ability may be granted to individuals or groups and may be for a single site or a group of sites. The purpose of this authorization is to ensure that downloads are for business purposes, and to minimize the impact of such operations on the overall network. This authorization also exists to prevent users from downloading and implementing beta software that has the potential to crash their system and/or the network.

News Groups (UseNet News) capabilities will be authorized by the TMD. These may also be granted to an individual or group and may be for a single or multiple user group. The purpose of this authorization is to ensure that access is for business purposes and to minimize the impact of such operations on the overall network.

3.6.1 ABUSE OF THE INTERNET OR INTRANET
Use of the internet or intranet by engaging in prohibited acts may result in disciplinary action up to and including termination.

3.6.2 SECURITY, PUBLIC RECORDS, AND BLOCKED ACCESS
The TMD will provide for internet security, which includes, but is not limited to, firewall protection, specific routing, profiles, and passwords.

Specific websites that have no legitimate business purpose will be blocked from access.

An audit trail of access to sites may be maintained by the TMD to investigate possible violation of City policy or breach of security. Such violations will be reported to the Chief of Police and the City's Chief Administrative Officer for appropriate disciplinary action.

3.6.3 INTERNET CONNECTIONS OUTSIDE OF THE CITY SYSTEM
During the course of an investigation, a detective may be required to visit a website that is currently “filtered” by the City of Orlando’s TMD. Computers have been assigned to the Criminal Investigations Division, Intelligence Unit, Special Victims Unit, and the Digital Forensic Lab to assist with these investigations.

Each detective who has access to these computers will have a screen name and password. The screen name and password shall be confidential with only the assigned detective(s) and the unit supervisor having knowledge of them. The password shall be changed when the detective(s) assigned to such investigations or the unit supervisor leaves one of these units.

Each computer will be assigned a log. The detective(s) assigned to work these investigations will document the date and time signed on and off the computer and the reason for the investigation. The unit supervisor will maintain, inspect, and initial the log monthly.

3.7 EMAIL
All employees with computers capable of internet access will be granted internet email access unless specifically denied by their bureau commander or the Chief of Police.

Employees may not use the City’s email system in any way that may be seen as insulting, disruptive, or offensive by other persons, or harmful to morale. Use of the City’s internet and intranet to access any site or material that is sexually explicit, pornographic or obscene, or that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, or religious or political beliefs, or that has the potential to cause the City public harm or disrepute, is strictly prohibited.

3.7.1 ACCESSIBILITY OF EMAIL
The City’s email system is installed for the purpose of facilitating official City business. The system belongs to the City and the contents of email communications are accessible at all times by the City for any business-related or other purpose. These systems may be accessed at any time, with or without advance notice. Although an employee may have a personal password, email can be accessed by the City without an employee’s knowledge or consent. Nothing on the email system, therefore, should be considered confidential. Moreover, all email messages are subject to public records law and will be disclosed upon request in accordance with the law's provisions.

3.7.2 RETENTION OF EMAIL
3.7.2.1 EMAIL PRIOR TO DECEMBER 1, 2010
Each employee is responsible for ensuring proper retention of email messages in accordance with the public records law for all email records dated prior to December 1, 2010. The TMD does not retain a central repository of these messages.

Public record email can be deleted after it has been retained for the correct time period as determined by the public records retention schedules. A public record that is stored and accessible after this time is still a public record and must be produced upon request. A systematic deletion program not only eliminates obsolete documents from the files, but also saves resources by not indefinitely and unnecessarily storing information beyond appropriate timeframes.

Employees must set up their own retention procedures to ensure compliance with the public records law. While methods for reviewing, storing, or deleting email vary, employees may comply with retention requirements of the public records law by doing one of the following:

a. Print the email and store the hard copy in the relevant subject matter file as any other hard-copy document. Printing the email permits the information on a particular subject matter to be maintained in one central location, enhancing its historical and archival value. The employee must also determine if the incoming email must be printed before being deleted from his or her system.

b. Electronically store public record email on the computer system and retain it electronically pursuant to retention schedules. Generally, correspondence, inter-department memoranda, and most fiscal and budget records must be retained for three years. Other items such as routine announcements, meeting notices, and the like are retained until the administrative purpose is served. Any questions regarding retention can be directed to the Records and Archives Manager in the City Clerk's Office.

3.7.2.2 EMAIL ON OR AFTER DECEMBER 1, 2010
Email generated on or after December 1, 2010, will automatically be archived and stored by the TMD for a period of 60 months from the date of the email. Employees will no longer be responsible for archiving their email dated on or after December 1, 2010.

3.8 CRIMINAL JUSTICE COMPUTER NETWORK (CJNET)
Access to the Criminal Justice Computer Network (CJNET) will be granted to all employees with the computer technology capable of executing the program unless specifically denied by their bureau commander or the Chief of Police. Access to the specific databases contained within the CJNET will be granted based on the individual's ability to demonstrate a legitimate need.

Requests for access to specific data bases within CJNET (i.e., AFIS, GANGNET, etc.) shall be forwarded in memo form to the supervisor of the Intelligence Unit for approval. These requests should convey the user's proposed need for the service and be endorsed through their section commander. Final authority for approving the requests will rest with the Investigative Services Bureau Commander.

The Intelligence Unit will maintain, in a secure location, all records regarding electronic certificates held by members of the Department.

3.9 MOBILE COMPUTERS
Mobile computers are utilized by various operational and administrative personnel throughout the Department. The type of mobile computer assigned and software accessed will vary according to the employee's organizational position and need. The general information that follows applies to all mobile computer users unless specifically noted for an MCT. Additionally, policy for MCT users is noted in section 3.9.11.

3.9.1 ASSIGNMENT
The Mobile Computer Coordinator shall assign the computer and its accessories. The employee to whom the mobile computer is assigned shall be personally responsible for the mobile computer and peripheral devices (power cords, car adapters, CD drives, floppy drives, etc.) and any loss, damage or misuse that may occur to these components. Personnel shall not lend, borrow or otherwise take control of any other user's mobile device without the approval of the Mobile Computer Coordinator.

Upon reassignment (including long-term restricted duty), activation for military duty or resignation/retirement, the employee shall return the computer and its accessories to the Quartermaster Unit. If the device is an MCT, the computer mount key shall be left on the vehicle key ring, which shall be turned in to the Quartermaster Unit when the vehicle is turned in for reassignment.

3.9.2 MOBILE COMPUTER CAPABILITIES
Mobile computers will provide the Orlando Police Department with a multitude of capabilities. These capabilities may include, but are not limited to:

a. The capability to conduct all routine business (i.e., service requests).
b. Internet/intranet access.
c. Access to City email.
d. Access to Mobile Messaging and Mobile Field Reporting software for the purposes of:
    1. Dispatching of all non-priority calls for service.
    2. Car-to-car messaging.
    3. Field access of NCIC/FCIC records.
    4. Self-initiating calls via the MCT.
e. Access to Crash Reporting
f. Field access to AS400 functions.

3.9.3 TRAINING
Only employees who have completed formal training on the use and operation of the mobile computers will operate the equipment.

3.9.4 OFFICER SAFETY
Although the mobile computers will reduce radio traffic by allowing tasks to be performed off the air, emergency calls will continue to be dispatched via radio. Additionally, members needing emergency assistance or having concerns about officer safety will utilize the radio system to make requests.

3.9.5 DRIVING WHILE USING MOBILE COMPUTERS
Mobile computers will only be used in vehicles with proper vehicle computer mounts. Officers shall ensure that they have the correct computer mount key for their vehicle and shall lock their mobile computer in the computer mount prior to starting the vehicle. For safety concerns, the use of a mobile computer while the vehicle is in motion is not advisable. Employees shall always ensure that the safe movement of the police vehicle is paramount and in keeping with the current issue of P&P 1802, Use of City Vehicles, and state laws.

3.9.6 PREVENTION OF DAMAGE OR THEFT
Special care will be taken to prevent damage to the units. Employees will use due care when handling the mobile computers including the MCTs. These units should not be exposed to excessive moisture (rain or spilled drinks) or intense heat. When transporting an MCT, the lid shall be securely closed. If an MCT is in the computer mount, it should be securely locked.

Non-ruggedized computers shall be transported in the designated carrying case. Employees shall not write on or affix decals, photographs, or other items to the computers.

3.9.7 DOCUMENTING LOST OR DAMAGED MOBILE COMPUTER AND/OR ACCESSORIES
When an employee is aware of a lost or damaged mobile computer or its accessories, they shall immediately notify their supervisor. The employee shall complete an incident report documenting the incident. The employee's supervisor shall complete an online Risk Management report. Loss or damage shall also be reported to the Mobile Computer Coordinator as soon as possible during normal business hours. The employee has the option to purchase replacements for lost or damaged items. The supervisor shall refer to the current issue of P&P 1604, Section 3, Responsibility of Investigation. Employees shall adhere to the policy set forth in Regulation 500-1, Department Property and Equipment and the current issue of P&P 1604, Discipline.

3.9.8 HIT CONFIRMATIONS
When an FCIC, NCIC, or local hit is received via mobile computer, confirmation will be obtained from Teletype via radio or telephone.

3.9.9 PUBLIC RECORD
Since transmitted information is recorded and open to public record requests, transmission made on the MCTs will be of the same nature as that transmitted on the radio. Profanity, "street jargon" or derogatory remarks will not be used or transmitted.

FCIC/NCIC information shall not be electronically copied to any officer-generated report or electronic communication. These may include, but are not limited to:

a. Call Narrative Updates
b. Arrest Affidavits
c. Warrant Arrest Affidavits
d. Report Case Narrative/Supplements
e. Car-to-Car or Car-to-CAD Messaging
f. Email
g. Crash Reports
h. Field Investigative Reports (FIR)

3.9.10 MOBILE COMPUTER TERMINALS (MCTs)
3.9.10.1 APPLICATION USER ACCOUNTS AND PASSWORDS
Each operator of the MCT will log on and off at the beginning and end of each tour of duty.

3.9.10.2 INFORMATION SECURITY
To secure restricted police information from public view, employees shall close the lid or use the "HIDE" feature in Mobile Messaging on the MCT, upon exiting their assigned vehicle (34.06c). Employees shall prevent any CJIS information displayed on the MCT from being read by non-law enforcement passengers in their vehicles.

3.9.10.3 FIELD OPERATIONS AND USAGE
MCT functions shall be based upon the discretion of the officer, taking into account officer safety considerations, emergency or other extenuating circumstances that would make the use of the MCT unsafe or impractical.

Officers will utilize the MCT as their primary means of receiving, responding to, and clearing their routine calls for service. MCT users will keep routine voice traffic to a minimum.

Officers may self-initiate via the MCT by utilizing the self-initiated feature in the Mobile Messaging application.

The following incidents shall not be self-initiated via the MCT and must be transmitted to Communications via the police radio:

a. Vehicle Stops
b. Suspicious Incident(s)
c. Suspicious Person(s)
d. Unknown Trouble
e. Disturbances
f. Incidents requiring medical personnel or additional units
g. Any transport of prisoners or citizens

Officers shall only self-assign themselves to an active call via the MCT by utilizing the self-assign feature in the Mobile Messaging application as a secondary unit.

Officers will enter their own call notes and dispositions except in exigent circumstances, such as being called to a critical call.

3.9.10.4 DEADLINING
3.9.10.4.1 VEHICLE
When deadlining a vehicle, the officer's assigned MCT shall be removed and maintained in the officer's possession or stored in a secure location. Under no circumstances shall the computer be left in the vehicle or trunk.

3.9.10.4.2 MCT
When an MCT is malfunctioning, users shall follow the procedure outlined in section 2.2, Help Desk. Prior to deadlining the MCT at Supply, all incomplete mobile field reports shall be returned to the server.

3.9.10.4.3 SPARE MCTs
If an assigned MCT must be deadlined for repair, the employee may check out a spare MCT from the Quartermaster Unit. The spare MCT shall be returned at the end of the employee's shift so it will be available for use by other officers. Prior to returning the spare MCT to the Quartermaster Unit, all incomplete mobile field reports shall be returned to the server. Employees who do not have an assigned MCT will not be allowed to check out spare MCTs. Exceptions to this policy may be made by the Mobile Computer Coordinator.

4. TELEPHONES

4.1 VOICE MESSAGE (VOICE MAIL)
Voice message processing, voice mailboxes, or phone mail will be used for City business purposes only. Evidence of abuse or misuse will constitute grounds for removal from the voice message processing system.

Voice message processing statistical reports will be monitored monthly for current and past activity as well as the security of the system. Suspected abuse or misuse will be reported to the TMD Chief Information Officer and the Chief of Police for disposition.

Employees desiring a voice mailbox will submit their requests in writing, using the Technology Management Service Request Form (Attachment B) via an OPD TBA. Bureau commanders will screen requests for appropriateness, need, and approval. A "MUST-ANSWER" phone number shall be provided on the form next to "Voice Mail" before entry into the phone mail system.

The employee's record will be removed from the phone mail system upon termination of employment, transfer to another office, or loss of the employee's services for a period of 30 days or longer.

The Telecommunications Manager will handle the operation and administration of all matters pertaining to the voice message processing system.

Persons using the phone mail system shall report all instances of trouble, busy signals, locked mailboxes, and evidence of misuse to the HELP DESK at 407.246.2600.

4.2 LONG DISTANCE TELEPHONE SERVICE
Long distance telephone service will be used for City business purposes only. Every effort will be made to contain calls to five minutes or less. While this guideline will at times be impractical, it shall be observed whenever possible. Callers misusing the long distance service are subject to appropriate disciplinary action. Long distance telephone service should NOT be used for the following:

a. Toll-free numbers (800 area codes)
b. Local numbers
c. Personal calls

Departments/bureaus are encouraged to obtain and use any toll-free numbers available from vendors, suppliers, and other contacts.

5. CELLULAR TELEPHONES

5.1 ASSIGNMENT OF CELLULAR TELEPHONES
Cellular telephones shall be issued to an individual if the member is the rank of sergeant or above. They may also be issued to a position/assignment (e.g., Homicide Detective, Fleet Coordinator, etc.) with approval of the Chief of Police. Approval of cellular telephone use may be affected by changes to the position, but not by the transfer of personnel. Program managers shall be responsible for the total number of cellular telephones assigned to their programs.

5.2 CITY BUSINESS
Cellular telephones shall be used for City business purposes only. Every effort shall be made to limit calls to ten minutes or less. While this guideline will at times be impractical, it shall be observed whenever possible. Cellular telephone usage shall be reviewed by the supervisor for evidence of misuse.

5.3 MISUSE
Callers misusing cellular telephones are subject to appropriate disciplinary action.

5.4 PERSONAL USE
Employees are expected to exercise good judgment while using the cellular network. Personal calls to or from a City cellular telephone are strongly discouraged. Such calls constitute "improper use of City equipment, supplies, or communication" as defined in City personnel policies. Occasionally, personal calls may be necessary, but frequent and/or repeated use of the cellular telephone may result in revocation of the cellular telephone use and/or disciplinary action.

5.5 CONVERSATION SECURITY
Cellular telephones are not “secure” devices. Conversations over cellular telephones can be overheard for up to a quarter of a mile by use of a radio receiver tuned to the proper radio frequency.

All numbers called on cellular telephones are a matter of public record. Calls to confidential witnesses or informants should be carefully weighed.

5.6 CELLULAR TELEPHONE VERIFICATION
The City’s contracted cellular provider will provide courtesy copies of monthly billing invoices. Program managers shall review these invoices with cellular telephone users to ensure that proper usage and billing is occurring. They shall also verify any international long distance telephone calls or text charges with the telephone user. Billing discrepancies shall be investigated and resolved.

5.7 PAYMENT FOR PERSONAL CALLS
Personal calls, cellular or long distance, and personal texting are strongly discouraged. Such calls constitute "improper use of City equipment, supplies, or communication systems" as defined in City personnel policies. Occasionally, personal calls and text messages may be necessary, but frequent and/or repeated use of the cellular/long distance services for such calls/text messages will be considered abuse and may result in disciplinary action and reimbursement to the City by the employee for actual costs incurred.

Employees shall reimburse the City for all personal international long distance calls and text messages, payable to the City of Orlando, and will be reimbursed at actual cost incurred. Payment will be made at OPD’s Fiscal Management Section.

5.8 CLONING, THEFT, OR LOSS OF CELLULAR TELEPHONES
In the event that a cellular telephone is cloned, lost, or stolen, the telephone user shall notify the TMD Help Desk by calling 407.246.2600 within 48 hours of the incident. In all instances, it will be the responsibility of the unit supervisor to ensure that this procedure is completed, unless it involves a cellular telephone assigned to a manager. In such instances, it shall be the manager’s responsibility to make notification to the TMD Help Desk.

5.09 INOPERABLE CELLULAR TELEPHONES
Cell phones that become inoperable shall be reported to the TMD Help desk by calling 407.246.2600. The TMD Cell Phone Administrator shall make the determination to replace or repair the phone and may direct the user to the City's contracted cellular telephone support vendor.

5.10 CELLULAR TELEPHONE ACCESSORIES
Cellular telephone users who require new or replacement accessories for their assigned City cell phone (i.e., holsters, chargers, etc.) shall submit a requisition to OPD Supply.

5.11 NEW CELLULAR TELEPHONES
All requests for new cellular service must be approved by the Chief of Police. Written approval will be forwarded to the OPD TBA, who will submit the work order. The TM Cell Phone Administrator shall purchase the necessary equipment and activate and assign the device. The phone shall be listed under the employee's equipment issued file by the Quartermaster Unit. All cellular telephone accessories shall be purchased/issued through the Quartermaster Unit.

5.12 TRANSFERS
When a transfer of personnel occurs, the employee being transferred shall notify the OPD TBA via email, who will in turn contact the TM Cell Phone Administrator. The OPD TBA shall determine whether the user may take their handset and phone number with them to the new position. When a transfer of personnel occurs and it is determined that the affected employee will no longer require a cell phone, the employee being transferred shall return the cell phone and all accessories to the Quartermaster Unit to be reissued.

5.13 RETIREMENT
When an employee with an assigned City cell phone retires, they shall return the cell phone and all accessories to the Quartermaster Unit to be reissued before they check out.

6. FACSIMILE MACHINES

Department facsimile machines shall be used for official police business only. They may be used when mailing is impractical. Department facsimile machine numbers shall be given out for official Departmental business only.

Any person who operates a facsimile machine must receive instructions on how to use the machine before attempting any first time transmissions. Operational instructions will be posted nearby.

Transmissions shall be made on the long distance telephone service when accessing long distance numbers. (9 + 1 + ten-digit number). Other local transmissions may be sent by dialing 9 + ten-digit number.

All facsimile transmissions shall be sent with an OPD fax transmittal cover sheet (Attachment C – available on the Word Add-ins Menu under Administrative Forms) specifying receiver of the document. Operators should advise sending parties to use a cover sheet to specify the name and unit to whom the document is to be delivered.

The manager responsible for each facsimile machine shall designate an employee responsible for collecting incoming facsimiles not immediately retrieved by the recipient. Any facsimile not retrieved within 24 hours shall be mailed to the recipient.

Any misuse or unauthorized use of the facsimile machine shall be reported to the operator's commanding officer.

The OPD Property Supervisor will individually tag facsimile equipment with City asset numbers. The OPD TBA will forward the appropriate documentation to the Telecommunications Manager. Facsimile equipment is not to be part of any individual department/office/bureau communications system.

Requests to purchase, replace, upgrade, or move facsimile equipment must first be coordinated through the OPD TBA.

7. PAGERS

Department employees are issued alphanumeric pagers based on their job assignment. Employees assigned a pager will have that pager available when on duty, or when notified to be on standby. Alphanumeric pagers have automatic statewide capability.

Employees issued alphanumeric pagers may receive written messages, which are initiated through the AS400 or the internet. Employees initiating messages to alphanumeric pagers are reminded that messages sent to City pagers are public record. Non-tactical pages shall not be sent out prior to 1530 hours (unless approved by a division commander) in an effort to avoid being disruptive to the personnel assigned to the midnight shift.

7.1 ISSUANCE OF PAGERS

Employees instructed by their chain of command to obtain a Department pager will obtain the pager from the OPD Communications Radio Systems Administrator.

7.2 PAGE TO CELLPHONES

In lieu of carrying a pager, employees may choose to have their pages sent to their City and/or personal cell phones or email accounts. If the employee elects this option and currently has an assigned pager, the employee shall turn the pager in to the Quartermaster Unit. Members assigned to a special team (i.e., SWAT, ESU, ERT, etc.) must keep and carry their assigned pager.

7.3 INOPERABLE PAGERS

Pagers that become inoperable may be replaced by contacting the OPD Communications Radio Systems Administrator.

7.4 PAGER GROUPS

MANAGER LEO – Used to communicate with members of the OPD Management Staff (i.e., civilian managers, lieutenants, and above).

NON-TACTICAL – All OPD employees assigned a City pager (all officers and civilians). Pages require authorization of a lieutenant or above. Authorizing name and contact number must be included in page. Pages can only be sent after 1530 hours. Division commanders or above can authorize pages prior to 1530 hours.

OPD CHIEF STAFF – Members of the Chief's Staff only. Programming of this group into a pager requires written authorization of the Chief or a designee.

OPD STAFF – Used to communicate with OPD managers, supervisors, Internal Affairs officers, as well as certain other City managers, of events such as computer outages, other system outages, road blockage, and other non-critical public safety incidents. Pages require authorization of a lieutenant or above. Authorizing name and contact number must be included in page.

OPD STAFF LEO – Used to communicate to OPD managers, supervisors, CAO, and DCAO of Law Enforcement Sensitive Staff pages. Pages require authorization of a lieutenant or above. Authorizing name and contact number must be included in page.

OFF DUTY – Used for the sole purpose of communicating extra-duty employment related information such as late notice extra-duty work opportunities, cancellations, issues, etc. Such information will no longer be transmitted to any other pager group. Participation in this group is entirely voluntary. Officers who choose to add this group to their pager understand and accept that such pages can be sent ANYTIME 24/7/365.

8. VIDEO CAMERAS

8.1 USES

Video cameras are extremely versatile and can be used effectively in a multitude of law enforcement operations, e.g., DUI enforcement, drug surveillance and enforcement activities, traffic control, and civil disturbances. Employees are reminded that public records or evidentiary law may require preservation and/or release of certain information

8.1.1 REMOTE VIDEO CAMERAS

This section applies to routine video monitoring and does not pertain to video cameras temporarily placed for a specific investigative purpose. For information related to the IRIS camera system, please refer to the current version of OPD P&P 1138, IRIS. For information related to supervisory review of video during a Response to Resistance investigation, please refer to the current version of OPD P&P 1128, Response to Resistance and Apprehension Techniques.

When video cameras are monitored from a remote location, the camera shall not be pointed at an angle that would view areas where there is a reasonable expectation of privacy nor have audio recording features activated unless authorized by court order. Signs will be posted that put citizens on notice that video cameras are present. Where cameras are attached to a recording device, the recordings will be maintained for a minimum of 30 days. If the recordings serve no investigative purpose, they will be recorded over or otherwise destroyed. Changing and maintenance of recordings will be controlled by the commander in charge of the facility where the monitoring and recording equipment resides.

8.2 CAUTIONS

Employees are cautioned that when recording video images, the use of the audio recording feature must meet the same standards as any other electronic audio interception. See Sections 1.4 and 8.5 for further details.

Employees are encouraged to employ department-approved cameras in any way that will enhance the police mission.

Video cameras are restricted to law enforcement and related activities and may not be used for personal or recreational purposes.

Employees shall not use personal or non-department-approved devices to capture moving images or video recordings of any type while acting in their official capacity. Such devices include any still cameras, digital cameras, cell phones, smart phones, or any video or audio recording devices, including vehicle-mounted (or adaptable) systems and/or body-worn (or carried) devices used for taking moving images or video recordings. For information related to permissible use of personal or non-department still cameras, digital cameras, cell phones, smart phones or similar devices for the collection and preservation of still photographic evidence only, please refer to the current version of OPD P&P 1902, Forensic Photography, Digital Cameras, and Digital Imaging Archive.

This policy does not prohibit the lawful collection of surveillance video taken by privately owned surveillance systems, e.g., bank or store owned surveillance video.

In rare or unforeseen circumstances (such as the capture of breaking events or the complete malfunction of department-approved equipment) any employee who creates or comes into possession of such record(s) is responsible to adhere to all evidentiary and Public Records retention requirements, including attachment or submission to any applicable case investigation(s). Such images or records shall not be deleted. The existence of these records shall be documented in a report.

Any record created or received in the course of the official business of the agency is subject to Florida's Public Records Law, and may also be considered evidence.

8.3 GENERAL ENFORCEMENT MEDIA

Blank, general use recording media shall be provided by the Quartermaster Unit and shall be used to record department-approved enforcement activity only.

8.4 DUI ENFORCEMENT MEDIA

If a DUI arrest is recorded, all recordings become evidence of the traffic stop, interview, field sobriety test, etc., and shall be preserved by being placed into OPD Property and Evidence. If the recording is made on a Department In-Car system, that recording uploads automatically onto the server for preservation. Officers requiring copies of such recordings must make a request for each copy needed.

Orange County Breath Technicians shall store any media they create for presentation in court. Employees shall ensure that any recorded media submitted as evidence does not contain any material unrelated to that particular case.

8.5 LEGAL CONSIDERATIONS

In order to minimize potential criminal and civil liability, employees using department-approved video or still cameras shall:

a. Only record or photograph individuals from areas open to the public, or private property or premises from which the owner or custodian of the property authorizes the employee to record or photograph.

b. Not use video camera enhancement devices (for example, telephoto or night-vision lenses) to record individuals located in private areas such as offices, residences, and other areas not open to the general public.

c. Use audio pick-up and recording features of a video camera or audio recorder only in furtherance of a legitimate law enforcement purpose, and:

    1. Where the employee has obtained the written consent of the person being recorded, or
    2. Where the employee, or an individual acting under the direction of the employee, initiates and is engaged in a conversation with the subject upon whom the video and audio features of the video camera are focused and such conversation is in furtherance of a criminal investigation, or
    3. Where the person being audio recorded does not have a reasonable expectation that his or her conversation is private.

If an employee desires an exception from the foregoing restrictions, he or she must contact the Police Legal Advisor who will assist in the procurement of a court order authorizing the desired video and/or audio recording.

8.6 VIDEO CAMERA INVENTORY

The Department no longer maintains a video camera inventory for temporary checkout. Members requiring video recording shall coordinate with either those units that have assigned cameras and/or systems, or the Forensic Video Analyst.

9. DIGITAL/TAPE RECORDERS

Digital/tape recorders and recordings are used by units throughout the Department. Issuance of audio recorders will be determined by the appropriate division commander. Employees are reminded that audio-recording conversations without the knowledge and permission of the other parties is a criminal act, unless the person has no reasonable expectation of privacy or the officer or informant is acting in the course of an investigation. Employees shall ensure they are aware of current laws and policies concerning covert tape recordings before taking such actions. For specific situational questions, employees are encouraged to contact the Police Legal Advisor before making such recordings.

ATTACHMENT A

MCT DEADLINE CARD

Date: _____ Time: _____

MCT Asset #: _____

Officer: _____

Emp#: _____ Shift: ___ Rotation: ___

Phone: _____ (Best number to reach you if questions)

- Help Desk Problem #: _____
- If damaged, which forms were completed?
  _____ Inc. report _____ Risk Mgmt report
- Power cord turned in: _____ Yes _____ No
  Note: only turn in if there is a problem with it.
- Please do not deadline your MCT with incomplete reports on it. Return incomplete reports to the server by saving them as incomplete.

PROBLEM: _____

(Use back of form, if necessary, to provide as much detail of problem as possible)

ALL MCTs MUST BE SIGNED IN/OUT OF COMPUTER LOG

Sample

ATTACHMENT B

Technology Management
Service Request

TM Project #: Related Project #:

Name:		**Employee #:**		**Rank:**	
Submitted by:		**Phone #:**		**Date Submitted:**	
Program # / Name:				**Effective Date:**	

Please provide 2 weeks notice for moves or changes. Large moves or installations may require 6 weeks notice.

Reason for request:	☐ New Hire ☐ Permanent Transfer ☐ Temporary Transfer ☐ Separation ☐ Other:	Describe functional need and justification for this request:

From		**To**	
Position Information:			
Program #:		Program #:	
Division:		Division:	
Section:		Section:	
Unit #:		Unit #:	
Unit Name:		Unit Name:	
Location/floor:		Location/floor:	
Phone #:		Phone #:	
Whose place will this person be taking in their new position?			
Name:		Emp #	
Position Title:			
For sergeants only: Who was your ASL?	Name:		Emp#:
Who will be your ASL?	Name:		Emp#:
Computer Information:			
Please note that all new laptop information should be verified with the Mobile Computer Administrator prior to the submission of this request.			
Asset #:	☐ Laptop ☐ Desktop	Asset #:	☐ Laptop ☐ Desktop
Make:	Model:	Make:	Model:
Jack #:	☐ Voice ☐ Data	Jack #:	☐ Voice ☐ Data
Telephone Information			
Previous Extension:	New Extension:		New Jack #:
Special Instructions:			
AS400 Information:			
Main Menu:		Main Menu:	
Authority:	☐ Employee/Officer ☐ Supervisor/ASL	Authority:	☐ Employee/Officer ☐ Supervisor/ASL
Printer Name:		Printer Name:	
Print Queue:		Print Queue:	
Job Queue:		Job Queue:	
Other Notes:			
Field Reporting Information:			
Field Reporting & ICJIS Authority:	☐ Employee/Officer ☐ Supervisor/ASL	Field Reporting & ICJIS Authority:	☐ Employee/Officer ☐ Supervisor/ASL
Windows Information:			
Network Folder(s):		Network Folder(s):	
Windows Printer(s):		Windows Printer(s):	
Color Printer(s):		Color Printer(s):	
Specialty Software Needed:			

Sample

ATTACHMENT C

Orlando Police Department
Enter your division or unit name here
100 South Hughey Avenue
Orlando, Florida 32801
407.246.
fax 407.246.

Fax Transmittal

To: **Fax:**

From: **Date:**

Re: **Pages:** (including cover)

Notes:

Sample

ORLANDO POLICE DEPARTMENT