"Keep Orlando a safe city by reducing crime and maintaining livable neighborhoods."

ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE

1625.8, USE OF ELECTRONIC COMMUNICATIONS SYSTEMS

EFFECTIVE DATE:	5/21/2025
RESCINDS:	P&P 1625.7
DISTRIBUTION GROUP:	ALL EMPLOYEES
REVIEW RESPONSIBILITY:	PROFESSIONAL STANDARDS DIVISION COMMANDER
ACCREDITATION STANDARDS:	26
RELATED LAWS:	N/A
RELATED POLICIES:	City Policies 754.6, 754.7, 754.10, 754.11
CHIEF OF POLICE:	ERIC D. SMITH

CONTENTS:

1. PURPOSE

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

2. 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.

3. DEFINITIONS

N/A

4. PROCEDURES

4.1 GENERAL

4.1.1 COMMUNICATIONS 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. Telephones, cellular telephones, voice mail, and facsimile (fax) devices.

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.

4.1.2 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 4.1.5 of this policy. Employees are reminded that public records or evidentiary law may require the preservation and/or release of certain information.

4.1.3 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. Before initiating such action, employees must ensure they are acting within current court rulings. Up-to-date information may be obtained through OPD Legal 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 the preservation and/or release of certain information.

4.1.4 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 the Information Technology (IT) AND their respective Bureau Chief.

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 Bureau Chief and Information Technology (IT) 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 Department Interface, Information Technology (IT).

The use of another's credentials (User ID and password) for computer or software application access is strictly prohibited.

4.1.5 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, 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.

4.2 SUPPORT

4.2.1 DEPARTMENT INTERFACE, INFORMATION TECHNOLOGY (IT)

Normally, the Orlando Police Department's technical equipment, applications, and support originate through Information Technology (IT). To facilitate more efficient support of technical needs, two Department Interfaces, have been assigned to support OPD. DI's acts as a liaison between OPD and IT to coordinate projects and resources. IT 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 OPD DI.

4.2.2 HELP DESK

The Help Desk is managed by the City's IT at City Hall. Help Desk personnel respond to issues concerning desktop computers (PC), mobile computers, printers, the computer network, and telephone 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 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.

4.2.2.1 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 1900 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").

4.2.2.2 AFTER HOURS SUPPORT

IT 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 IT 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 immediate on-site or escalated support for essential services (e.g., IT-supported CAD, ICJIS, Teletype, etc.).

4.2.3 IT CELL PHONE ADMINISTRATION PROCESS

The IT OPD employee designated as the Cell Phone Administrator shall be the Special Projects/Technology Liaison and is responsible for the service and technical support of all OPD cellular telephones and any 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 Special Projects/Technology Liaison first, and if unavailable the user can contact the Help Desk by calling 407.246.2600.

4.2.4 TRAINING

The City's IT coordinates vendor-led 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.

4.3 COMPUTER HARDWARE AND SOFTWARE

4.3.1 DEFINITIONS

CREDENTIALS: Refers to the user ID and password for any computer/software application. Credentials are confidential and should not be shared with anyone.

MOBILE COMPUTER: shall include any laptop or tablet computer with wireless connectivity.

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

MOBILE COMPUTER COORDINATOR: The designated OPD Special Projects/Technology Liaison shall serve as the Mobile Computer Coordinator, providing inventory support for all OPD mobile computers.

IT UPDATER: is software developed and utilized by IT to remotely send updates to OPD computers.

4.3.2 COMPUTER ACCESS/SECURITY

4.3.2.1 AUTHENTICATION

All OPD computers use dual authentication (two logins/biometrics) to confirm authorized access to police data. This complies 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 (username and password) and multi-factor authentication method to sign on or authenticate to the OPD computer network.

4.3.2.2 USER ACCOUNT SECURITY

Users should lock their computers when leaving when on and unattended.

4.3.2.3 VIRUS CONTROL MEASURES

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

4.3.3 COMPUTER FILES MAINTENANCE, BACKUP, AND RETENTION

IT will ensure the applications and data, including but not limited to the Computer Aided Dispatch (CAD) system and the Law Enforcement Records Management System (LERMS) are replicated to a secondary datacenter using Site Recovery Manager (SRM). If LERMS fails to operate, IT personnel has the ability to switch production from LERMS to the fail-over environment.

Other networked OPD computer servers, including, but not limited to the N:\ drive, are fully backed up to an internal backup server on a nightly basis. The encrypted full backups are moved to an encrypted air-gapped location where they are stored for up to two weeks.

4.3.4 COMPUTER UPDATES

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

4.3.5 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.

4.3.5.1 OPD INTERNET

The Orlando Police Department currently maintains an internet presence for external customers through the City of Orlando's website Orlando.gov. The OPD 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 Relations 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, Orlando Police Website.

4.3.5.2 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 the completion of law enforcement duties.

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

4.3.6 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 the Chief of Police, their bureau commander, or designee.

All employees shall adhere to City Policy 754.10 Internet and Intranet Policy. 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 per the current version of P&P 1635, Social Media, and City of Orlando policy.

News Groups (UseNet News) capabilities will be authorized by IT. 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 access is for business purposes and to minimize the impact of such operations on the overall network.

4.3.6.1 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.

4.3.6.2 SECURITY, PUBLIC RECORDS, AND BLOCKED ACCESS

IT will provide for internet security, which includes but is not limited to, firewall protection, specific routing, profiles, passwords, and content filtering.

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 IT to investigate a 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.

4.3.6.3 INTERNET CONNECTIONS OUTSIDE OF THE CITY SYSTEM

During an investigation, a detective may be required to visit a website currently "filtered" by the City of Orlando's IT. Specific computers have been assigned to the Criminal Investigations Division, Intelligence Unit, Special Victims Unit, and Digital Forensic Lab to assist with these types of 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 knowing 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.

4.3.7 EMAIL

All employees are required to adhere to City Policy 754.11 Email, regarding the proper use of email messages sent or received by City employees using the City's Email system.

4.3.8 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 databases 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. The 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.

4.3.9 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, the policy for MCT users is noted in section 4.3.9.10.

4.3.9.1 ASSIGNMENT

The Special Projects/Technology Liaison shall assign the MCT 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, 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 Special Projects/Technology Liaison.

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. The device will be returned to the Special Projects/Technology Liaison for reissuing.

4.3.9.2 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 Computer Aided Dispatch (CAD) and Mobile Field Reporting software for:
    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. Access to LERMS

4.3.9.3 TRAINING

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

4.3.9.4 OFFICER SAFETY

Although using the mobile computer aims to 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.

4.3.9.5 DRIVING WHILE USING MOBILE COMPUTERS

Mobile computers will only be used in vehicles with proper vehicle computer mounts. Officers shall ensure they have the correct computer mount key for their vehicle and shall lock their mobile computer in the computer mount before 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 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.

4.3.9.6 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 a proper protective carrying case. Employees shall not write on or affix decals, photographs, or other items to the computers.

4.3.9.7 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 loss must also be immediately reported to IT by the responsible supervisor. The employee's supervisor shall complete an online Risk Management report. Loss or damage shall also be reported to the Special Projects/Technology Liaison as soon as possible during normal business hours, or via email after 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, Discipline, Section 3, Responsibility of Investigation. Employees shall adhere to the policy outlined in Regulation 500-1, Department Property and Equipment, and the current issue of P&P 1604, Discipline.

4.3.9.8 HIT CONFIRMATIONS

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

4.3.9.9 PUBLIC RECORD

Since transmitted information is recorded and open to public record requests, a 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)

4.3.9.10 MOBILE COMPUTER TERMINALS (MCTs)

4.3.9.10.1 APPLICATIONS USER ACCOUNTS AND PASSWORDS

Each operator of the MCT will log on and off at the beginning and end of each tour of duty.

4.3.9.10.2 INFORMATION SECURITY

To secure restricted police information from public view, employees shall close the lid or lock MCT using the Windows feature, 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.

4.3.9.10.3 FIELD OPERATIONS AND USAGE

MCT functions shall be based upon the discretion of the officer, taking into account officer safety considerations, emergencies, 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 CAD 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 CAD application as a secondary unit.

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

4.3.9.10.4 DEADLINING

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.

MCT
When an MCT is malfunctioning, users shall follow the procedure outlined in section 4.2.2, Help Desk. Before deadlining the MCT at the Quartermaster Unit, all incomplete mobile field reports shall be returned to the server.

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. Before 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 Special Projects/Technology Liaison.

4.4 TELEPHONES

4.4.1 VOICE MESSAGE (VOICEMAIL)

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. The Use of Voice Message Processing will be in accordance with City Policy 754.7, Request and Use of Voice Message (Voicemail) Processing.

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.

4.5 CELLULAR TELEPHONES

4.5.1 ASSIGNMENT OF CELLULAR TELEPHONES

Cellular telephones may 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 the approval of the Administrative Services Bureau Commander. 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.

4.5.2 CITY BUSINESS

Cellular telephones shall be used for City business purposes only. Cellular telephone usage shall be reviewed by the Special Projects/Technology Liaison for evidence of misuse.

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

4.5.4 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.

4.5.5 CONVERSATION SECURITY
Cellular telephones are not “secure” devices. Conversations over cellular telephones can be overheard for up to a quarter of a mile by the 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.

4.5.6 CELLULAR TELEPHONE VERIFICATION
The City’s contracted cellular provider will provide courtesy copies of monthly billing invoices. The Fiscal Management Section Manager or their designee shall review these invoices with the Special Projects/Technology Liaison to ensure that proper usage and billing are 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.

4.5.7 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 the actual cost incurred. Payment will be made at OPD’s Fiscal Management Section

4.5.8 CLONING, THEFT, OR LOSS OF CELLULAR TELEPHONES
If a cellular telephone is cloned, lost, or stolen, the telephone user shall notify the Special Projects/Technology Liaison immediately upon discovery during normal business hours, or via email after hours. 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 a notification to the Special Projects/Technology Liaison

4.5.9 INOPERABLE CELLULAR TELEPHONES
Cell phones that become inoperable shall be reported to the Special Projects/Technology Liaison via email. The Special Projects/Technology Liaison shall determine whether to replace or repair the phone and may direct the user to the City’s contracted cellular telephone support vendor.

4.5.10 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 the Quartermaster Unit.

4.5.11 NEW CELLULAR TELEPHONES

All requests for new cellular service must be approved by the Administrative Services Bureau Commander, but first routed to the Special Projects/Technology Liaison. If approved, the Special Projects/Technology Liaison shall purchase the necessary equipment and activate and assign the device. All cellular telephone accessories shall be purchased/issued through the Quartermaster Unit.

4.5.12 TRANSFERS

When a transfer of personnel occurs, the employee transferred shall notify the Special Projects/Technology Liaison via email, unless the member is transferring to a position authorized for a cellular telephone. When a transfer of personnel occurs and it is determined 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.

4.5.13 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.

4.6 FACSIMILE MACHINES

Department facsimile machines shall be used for official police business only. They may be used when mailing or email is impractical. Department facsimile machine numbers shall be given out for official Departmental business only. All employees shall adhere to City Policy 754.6, Request and Use of Facsimile Equipment regarding the proper and allowable use of facsimile machines.

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

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

4.7 VIDEO CAMERAS

4.7.1 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 the preservation and/or release of certain information.

4.7.1.1 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 Crime Center camera system, please refer to the current version of OPD P&P 1138, Public Safety Camera Network.

For information related to a supervisory review of video during a Use of Force investigation, please refer to the current version of OPD P&P 1128, Use of Force.

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.

4.7.2 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 4.1.4 and 7.8 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, smartphones, 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 the permissible use of personal or non-department still cameras, digital cameras, cell phones, smartphones, 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.

4.7.3 LEGAL CONSIDERATIONS AND PROHIBITED RECORDINGS AND ACTIONS

Unless conducting official law enforcement business that requires the member to use department-approved video or still cameras (recording devices), the following is a list that members must adhere to:

a. Recording devices will not be used to record personal activity.
b. Recording devices will not be intentionally activated to record conversations of fellow employees without their knowledge during routine, non-enforcement-related activities.
c. Recording devices will not be used to intentionally record confidential informants or undercover operations.
d. Unless the recording device is being used as part of an official law enforcement incident, the recording device will not be activated in places where a reasonable expectation of privacy exists, such as, but not limited to, locker rooms, dressing rooms, or restrooms.
e. Members will not make copies of any recordings for their personal use.
f. Members are prohibited from allowing anyone else to use another recording device to record media captured from the department-issued recording devices.
g. Members shall not erase, alter, reuse, modify, or tamper with any recording. Only the authorized MVSA may erase any previously-recorded digital recording.
h. Members shall not post recording device footage to any social media site without prior written approval from the Chief of Police or their designee.

i. Unless in response to an official inquiry or investigation, members will not allow citizens to review the recordings.
j. Members shall not lead a person to believe the recording device has been deactivated when, in fact, the recording device is left active.
k. No member shall use a recording device not assigned to them. Only authorized supervisors or MVSA can assign a recording device to a member.
l. Members shall not use recording devices to replace a written report or required written statements.

Juvenile School Location: Members shall not activate a recording device while on the grounds of any public, private, parochial, elementary, middle, high, or secondary school, except when responding to an imminent threat to life or where there is a potential for enforcement and/or criminal investigation.

Medical Facilities**:** Unless conducting official law enforcement duties, members shall not record patients during medical or psychological evaluations by a clinician or similar professional, or during treatment. Members shall be aware of patients' rights to privacy when in hospital settings. When recording in hospitals and other medical facilities, officers shall be careful to avoid recording persons other than the individual of interest.

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

4.8 DIGITAL RECORDERS

Digital 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 are 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 recordings before taking such actions. For specific situational questions, employees are encouraged to contact the Police Legal Advisor before making such recordings.

5. FORMS AND APPENDICES

ATTACHMENT A-MCT Deadline Card

ATTACHMENT B-Service Request Form

ATTACHMENT C-Fax Transmittal Cover