RECEIVED
JAN 29 2020
BOARD OF POLICE COMMISSIONERS

PLANNING, RESEARCH, AND DEPLOYMENT

TRANSMITTAL OF WRITTEN DIRECTIVE

FOR SIGNATURE OF: James E. Craig, Chief of Police

TYPE OF DIRECTIVE: Manual Directive 301.5

SUBJECT: MOBILE COMMUNICATION DEVICES

ORIGINATED OR REQUESTED BY: Planning, Research, and Deployment

APPROVALS OR COMMENTS:
The above referenced directive is a new directive. The information is this directive was pulled from the IACP Model Policy for Mobile Communication Devices and the City of Detroit Mobile Device Policy. This policy was reviewed and approved by Director Art Thompson of Technical Services.

Approved
12/26/19

APPROVED
ASSISTANT CHIEF
ADMINISTRATIVE OPERATIONS

AFTER THE DIRECTIVE IS APPROVED AND SIGNED, PLEASE RETURN TO PLANNING, RESEARCH, AND DEPLOYMENT.
1301 Third Street, 7th Floor, Detroit MI 48226

19-41 L

Series	Effective Date	Review Date	Directive Number
300 Support Services		Three Years	301.5
Chapter 301 - Communications			
Reviewing Office Technical Services			☒ New Directive ☐ Revised
References			

MOBILE COMMUNICATION DEVICES

301.5 - 1 PURPOSE

The purpose of this policy is to provide Department members with guidelines for the use of cellular phones as well as similar mobile communication devices, hereafter referred to as "MCDs." This policy does not cover the use of mobile computer terminals (MCTs).

301.5 - 2 POLICY

It is the policy of this Department to use MCDs in the course of police operations to enhance Departmental communication. MCDs may be used by members to conduct official business when the use of radio communication or landline telephones is inappropriate, unavailable, or inadequate to meet communication needs and when the device is used in accordance with this policy. Information or data housed in personal or Departmental MCDs related to the course and scope of employment is the property of the Detroit Police Department (DPD).

301.5 - 3 Definitions

301.5 - 3.1 Course and Scope of Employment

A Department member's work or actions, whether performed on or off duty, to further the Department's law enforcement responsibilities and goals as authorized by law; statute; or Departmental policies, procedures, rules, and training.

301.5 - 3.2 Disruptive Activity

Any time the MCDs would be considered disruptive, such as in meetings, training sessions, court, or public places when their use would reasonably be deemed inappropriate or intrusive.

301.5 - 3.3 Distraction

Any time the use of an MCD would divert, hinder, or delay the attention of a Department member from official duties and/or cause a potentially hazardous situation.

301.5 - 3.4 Mobile Communication Device (MCD)

Cellular telephones, personal digital assistants (PDAs), and any such device designed to record, transmit, and/or receive voice communications, text messages, e-mail, sound, video, or photographic images.

301.5 - 3.5 Personal Use

Use of an MCD, to include verbal conversations, texting, Internet use, game playing, and similar functions, that is unrelated to a Department member's official duties.

301.5 - 4 Procedures

301.5 - 4.1 Use of MCDs

1. MCDs shall be used only to conduct official police business while the member is on duty. Personal use is restricted and subject to Departmental review or supervisory approval.
2. MCDs are an augmentation to the Department's communication system, not a substitute for radio communication designated for transmission through the Department's emergency communication center. Approved uses include, but are not limited to, the following types of communications:

    a. Conveyance of sensitive or restricted information;
    b. Transmission of information related to undercover operations;
    c. Lengthy communication with other personnel on a Department-related matter;
    d. Communication beyond normal radio range; and
    e. Incidents in which use of a landline telephone would be appropriate but where one is not available.

3. Members should not normally provide the number of their MCDs to public citizens. Exceptions may be made when immediate future contact between a Department member and a victim, witness, or other person may be important.
4. Members shall not provide the MCD number of any other member of this Department to a public citizen without that member's authorization.
5. Members may not operate Department vehicles while using MCDs unless emergency circumstances exist and other means of communication are not available or suitable. When possible, members should pull off the roadway in a safe location when using MCDs unless hands-free operational devices are available.
6. Department-issued MCDs may be used in off-duty capacities only for the conduct of police-related business or during Department-related off-duty law enforcement assignments.
7. The records of MCD use, whether Department-owned or personal, while on duty may be subject to review by the Department.
8. DPD reserves the right to deny the use of any personal MCDs while the member is on duty. When authorized, members electing to carry personally owned MCDs while on duty must provide their immediate supervisor with the MCD's calling number.
9. Personal MCDs are governed by the same safety and use restrictions as provided above.

301.5 - 4.2 Use of Audio and Visual Recordings

1. Voice, text, or image recordings obtained during the course and scope of a member's employment, whether by personal or Department-issued equipment, are the property

of this Department and are governed by evidentiary policies of this Department, potential Brady disclosure requirements, and any public records retention and disclosure laws of this state.

2. Audio recordings of conversations may be subject to federal and state wiretapping laws.
3. The use of personal audio- or video-recording devices, where authorized by the Department, may be used to preserve perishable evidence when better options are not reasonably available. Members shall make their supervisor aware of any recorded information that is obtained during the course and scope of the member's employment or that may be reasonably considered germane to an investigation or other Departmental business.
4. No member will erase or attempt to delete, remove or alter any image, video, or audio file related to Department business or taken while on duty from an MCD unless authorized to do so by the Department.
5. Members shall not keep personal copies of any image, video, or audio file related to Department business.
6. Text, voice, or photographic images made in the course of conducting official police business, whether on or off duty, may not be shared with third parties in this Department or elsewhere, unless they have a need and a right to such information in order to further an investigation or conduct other official Departmental business.
7. Members shall not use MCDs to share messages or visual or audio recordings with social or other print or electronic media, when such communications could reasonably be considered positions of this Department, could undermine Departmental integrity, or bring disrepute to the Department or its members.

301.5 - 4.3 Security Requirements

Members shall ensure that the following security requirements are met for any Mobile Communication Device (MCD) that is used during the course and scope of employment:

a. Devices shall not be "jailbroken" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
b. Members shall not load pirated software or illegal content onto their devices. Applications shall only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. Any questions about the authenticity of an application or code shall be directed to the Public Safety IT department.
c. If a member suspects that unauthorized access to company data and information has taken place via a mobile device the member must report the incident to Public Safety IT immediately.
d. MCDs must be kept up to date with manufacturer or network provided patches. As a minimum, patches should be checked for weekly and applied at least once a month.
e. All MCDs must have approved virus and spyware detection/protection software along with personal firewall protection (where applicable).
f. The physical security of these MCDs is the responsibility of the member to whom

the device has been assigned. MCDs shall be kept in the member's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight.

g. If a mobile device is lost or stolen, promptly report the incident to the Public Safety Help Desk and the Commanding Officer of the member's unit. The member must document the serial number of the MCD.
h. MCDs must be encrypted in line with the City's compliance standards.
i. A "remote wipe" option must be available.

301.5 - 4.4 Mobile Device Management

Mobile Device Management (MDM) facilitates the implementation of sound security controls for MCDs and allows for centralized oversight of configuration control, application usage, and device protection and recovery. Public Safety IT shall ensure that all Department-Issued MCDs have MDM installed.

Related Policies:

- 102.8 Department Internet Usage/Web Pages/Social Networking
- 301.2 Telephones, Voicemail, and Cellular Phones
- 307.4 Criminal Justice Information Systems (CJIS)