HONOLULU POLICE DEPARTMENT

POLICY
LAW ENFORCEMENT OPERATIONS

June 10, 2015	Policy Number 4.16

MOBILE DATA COMPUTERS

POLICY

The Honolulu Police Department (HPD) shall maintain a mobile data computer (MDC) system that is supported by the necessary hardware, software, training, and guidelines for the general use and care of the MDCs.

PROCEDURE

I. DEFINITIONS

MDC: A department-issued, laptop computer that sends and receives data via a wireless data network and associated equipment, including antennas, aircards, etc. The MDC is configured to receive case information from the Computer Aided Dispatch System.

Log-on password: A password which allows a user to activate and access the MDC system.

II. USER INSTRUCTIONS

The department shall provide training in the use of the MDCs to personnel who are issued the units. This training shall be provided before personnel are permitted to use the MDCs for police work. While general guidelines are provided in this policy, use of the MDCs, including specific prohibitions, shall be in accordance with the training provided.

III. GENERAL USE

A. Only authorized departmental personnel shall use the MDCs. Personnel who require an MDC shall complete all necessary training before an MDC can be issued.

B. At the beginning of their tours of duty, officers who are issued an MDC and drive a fleet vehicle shall install the MDC into the mount, which holds the unit in place in the vehicle.

If a computer must be removed from a regular fleet vehicle, only the MDC shall be removed/released from the mount. Under no circumstances shall an officer remove any portion of the mount (e.g., post or brackets) along with the computer.

1. Each user shall log on at the beginning of the tour of duty and log off at the end of the tour of duty.

2. Each user shall utilize only his or her assigned log-on password.

4-4-2019

3. Whenever an MDC and/or MDC-related equipment is inoperable, the user shall call the Information Technology Division (ITD) MDC helpdesk for assistance (see the HPD intranet for contact information).

C. Confidential information that is contained or displayed on an MDC shall be kept out of view of nonlaw enforcement personnel.

1. The MDC should be secured or MDC screen cleared of any confidential information as soon as practicable before the user moves away from the MDC.

2. In the event that confidential information can be accessed from the MDC, including information stored on any portable storage devices, the employee shall ensure that the data is secure, even when the MDC is not in use. The department shall provide a means to protect the data, such as encryption or maintaining the data on removable media.

D. Authorized personnel shall confirm notifications of all temporary restraining orders, outstanding warrants, and outstanding auto thefts received via their MDCs before taking any law enforcement action.

E. Personnel shall not use the MDCs while operating vehicles that are in motion. In addition, personnel should not use the MDC in other situations where use of the MDC might compromise safety.

F. Both the MDC system and any display or communications via the MDC are the property of the HPD.

IV. ASSIGNMENT AND ISSUANCE OF MDCs

A. The assignment of the MDC shall be made or changed at the discretion of the ITD commander or designee.

B. The ITD will issue the MDC and associated portable computer equipment.

C. The MDC and associated portable, computer equipment shall be returned to the ITD when the employee separates from employment with the department.

When an employee transfers from a patrol to a nonpatrol element or other unit not authorized to use the MDCs, the MDC and associated portable, computer equipment shall be returned to the ITD within seven days of the transfer.

The ITD commander may grant an exception for extended special assignments upon receipt of a written request submitted by the employee via channels.

4-21-2017

D. Officers shall make every effort to submit police reports via the MDC or any desktop computer utilizing the Case Report System feature.

E. In the event that the MDC and/or associated portable, computer equipment is not working properly or has to be repaired, the employee shall call the MDC helpdesk to report the problem. If the MDC and/or any related equipment has to be replaced, as determined by the ITD, the employee shall submit the "Request for Replacement of Issued Item(s)" e-form via channels to the ITD with an e-form copy to the Finance Division.

F. During leaves of absence longer than 30 consecutive days (e.g., military leave, family leave, or suspension), the employee shall return the MDC and associated portable, computer equipment to the ITD prior to the leave commencing.

G. Personnel on medical/sick leave longer than 30 days shall return the MDC and associated portable, computer equipment to the ITD as soon as practicable.

H. If the employee is not able to return the MDC and associated portable, computer equipment, the employee's supervisor should assist the employee with returning the items to the ITD.

4-21-2017

I. In the event that an employee is away from a patrol assignment or on leave (i.e., military leave, special assignment, medical leave, etc.) for a period of more than one year, that employee shall attend an MDC refresher course taught by the ITD prior to being issued an MDC.

V. INSTALLATION

All permanent hardware installations, modifications, and removals shall be performed only by department-authorized personnel (e.g., personnel from the Telecommunications Systems Section [TSS], ITD Data Section, and the contracted vendor). Unless specifically authorized by either the TSS or ITD, no MDC user shall tamper with any part of the permanently installed hardware.

VI. TRANSACTION LOG, GLOBAL POSITIONING SYSTEM, AND AUTOMATED VEHICLE LOCATOR

A. The MDC stores transaction logs of Global Positioning System (GPS) data, criminal history checks, vehicle checks, rap and warrant checks, etc. These transaction logs shall be maintained in accordance with any applicable, established retention policies.

B. The GPS data obtained from the MDC is utilized by the Automated Vehicle Locator (AVL) system, which can display an officer's vehicle or MDC location on a map. The GPS data shall be used primarily for location-based dispatching and supervision and to enhance officer safety.

1. The GPS data shall not be used as the sole basis for any administrative investigation. However, the GPS data may be used to support or refute evidence in an administrative investigation.

2. The GPS data may be used for criminal or administrative investigations involving criminal misconduct.

VII. OTHER GOVERNING DOCUMENTS

A. The dissemination of information displayed, received, or transmitted via the MDCs is governed by Policy 2.21, STANDARDS OF CONDUCT, as well as other directives that address police records and data files, such as:

1. Policy 8.17, SECURITY AND HANDLING OF DEPARTMENTAL RECORDS AND FILES; and

2. Policy 8.20, COMPUTER SECURITY.

9-24-2018

B. The use of MDC hardware and software is also governed by guidelines established in Policy 8.08, USE OF COMPUTER HARDWARE AND SOFTWARE. Personnel shall not activate screen savers of any kind on the MDCs. Screen savers can interfere with an MDC's reception of emergency notifications.

C. Prohibitions in Policy 3.28, SEXUAL HARASSMENT, shall also apply to content of a sexual nature that is displayed or transmitted via the MDCs. In addition, personnel shall not display or transmit material that is sexist, racist, derogatory, vulgar, or discriminatory via the MDCs. These prohibitions do not include the creation, transmission, or display of material that is necessary for official investigative or reporting purposes. Supervisors are responsible for ensuring that each investigative or reporting use of such material is appropriate and authorized.

VIII. SECURITY

Employees are always responsible for the proper security of the MDCs that are assigned to them.

IX. CARE OF THE MDCs

To avoid spillage that can damage the MDCs, personnel shall take special care to keep liquids (such as soft drinks) and particles (such as food crumbs) and other debris away from the units.

As with other issued police equipment, the user is ultimately responsible for the MDC while the unit is in his or her care. This is also applicable to the storage of the MDC and any associated portable computer equipment. Therefore, the user shall exercise extreme caution and attention to ensure that the unit is not lost, stolen, damaged, or misused.

X. DAMAGES

A. With the exception of normal wear and tear, any damage to an MDC shall be documented by the officer who was responsible for the unit when the damage occurred. The officer shall initiate either a Miscellaneous Public case, which should cross reference any relevant reports (e.g., Motor Vehicle Collision report) or initiate the appropriate criminal case.

B. In the event that the MDC is lost or stolen, the employee or the employee's supervisor (if the employee is incapacitated) shall call the MDC helpdesk, as soon as practicable, to report the loss in order to preserve the security of the data and resources.

C. The employee shall file the police report and submit a copy of the report, via channels, as an attachment to the "Request for Replacement of Issued Item(s)" e-form.

SUSAN BALLARD
Chief of Police

4-4-2019

Post on bulletin board for one week

Policy first issued
April 28, 2000