

GENERAL ORDER



DISTRICT OF COLUMBIA

Subject Metropolitan Police Department Wide Area Network (MPDNet)		
Topic	Series	Number
SPT	302	08
Effective Date November 27, 2013		
Replaces: General Order 302.8 [MPDNet (Metropolitan Police Department Wide Area Network)], Effective Date March 16, 2011		
Rescinds: GOC-13-03 [GO-SPT-302.08 (Metropolitan Police Department Wide Area Network)], Effective Date June 21, 2013		
Related to: GO-SPT-302.09 (Use and Operation of Mobile Data Computers) GO-SPT-302.10 (Mobile Device Security)		

I.	Background	Page	1
II.	Policy	Page	1
III.	Definitions	Page	1
IV.	Regulations	Page	3
V.	Procedures	Page	9
V.A	Helpdesk Services	Page	9
V.B	Equipment Turn-in Requests	Page	10
V.C	Non-MPD User Access to the MPDNet	Page	10
V.D	Termination of Access to the MPDNet	Page	10
VI.	Roles and Responsibilities	Page	10
VII.	Cross References	Page	12

I. BACKGROUND

The purpose of this general order is to provide guidance to Metropolitan Police Department (MPD) members on the regulations and procedures for the use of MPDNet assets and services that are the property or responsibility of the MPD.

II. POLICY

It is the policy of the MPD to provide access to computer hardware and software to assist members with the performance of their duties to meet the mission of the MPD and to control information disseminated and accessed via use of the MPDNet in accordance with MPD policy and regulations, federal and local laws, and applicable licensing agreements.

III. DEFINITIONS

When used in this directive, the following terms shall have the meanings designated:

1. Computer System (Terminal) – Interconnected computers that share a central storage system and various peripheral devices such as a printer, scanner, or router.

2. Downloading – Process of transferring data or files from one (1) source to the memory of another device.
3. Hardware – Includes, but is not limited to, workstations, laptops, file servers, printers, peripheral devices, cable devices, routers, cabling infrastructure and telecommunication devices as defined in GO-SPT-302.11 (Telecommunication Devices).
4. Internet – Electronic communications network that connects computer networks and organizational computer facilities around the world.
5. Litigation Hold – Notice informing a member that litigation is pending or is anticipated and directing that member to preserve all relevant documents and to stop the routine document retention policies for such documentation.
6. Members – Sworn or civilian employees, MPD Reserve Corps members, contractors, summer youth employees, volunteers or others who are authorized by MPD to use MPD-owned or operated equipment and facilities.
7. MPDNet – Metropolitan Police Department Wide Area Network.
8. Obscene – Offensive to morality or decency; of utterly no redeeming social value, or a violation of contemporary national community standards.
9. Social Media – Category of Internet-based resources that integrate user-generated content and user participation including, but not limited to, social networking sites (e.g., Facebook, MySpace), microblogging sites (e.g., Twitter, Nixle), photo and video-sharing sites (e.g., Flickr, YouTube), wikis (e.g., Wikipedia), blogs, and news sites (e.g., Digg, Reddit).
10. Social Networks – Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.
11. Software – Applications accessed via MPDNet that may reside on file servers, mainframes, and other computers. Services include, but are not limited to, applications used to access the Internet, electronic mail (e-mail), and shared printing and file services.

IV. REGULATIONS

A. General/MPDNet

1. Members are reminded that they have no expectation of privacy while using MPD hardware. MPD hardware may be inspected or searched at any time, even when the hardware is assigned to, or used exclusively by, a single member.
2. Members shall access only the computer hardware and software which they are authorized.
3. Members shall submit requests for new computer software and hardware through the chain of command to the Chief Technology Officer (CTO), MPD-OCTO, for approval. Prior to granting authorization, the CTO, MPD-OCTO, or his/her designee, shall ensure compatibility with MPD technology standards and equipment and software operating on the MPDNet.
4. Members shall not install software onto MPDNet resources without first having the approval of the MPD-OCTO.
5. Members shall use all commercial software in accordance with applicable manufacturers' copyright and licensing agreements.
 - a. Members shall use software on the terminal/computer for which it was purchased and shall only use the software on one (1) system at a time unless a site license was purchased for the software.
 - b. Members who reproduce software illegally or who use illegally copied software may be subject to disciplinary action, civil damages and/or criminal penalties.
6. Members shall not alter, remove or relocate MPD computer hardware and software without prior authorization from MPD-OCTO.
7. Members shall limit incidental, personal use of the Internet (including e-mail transmission) to purposes that do not:
 - a. Directly or indirectly interfere with the operation of the MPDNet, computing facilities, or the MPD e-mail system.
 - b. Burden the MPD with noticeable incremental cost.
 - c. Violate the provisions of Part IV.D of this order.
 - d. Interfere with the member's duties or other obligations to the MPD or the District of Columbia Government.
8. The Department retains the right to restrict a member's ability to send email to large numbers of recipients (e.g., a police district distribution list) for other than official purposes.

9. Members shall not load or install MPD hardware or software onto personally-owned hardware (e.g., laptop computers, cellular phones) without prior authorization from MPD-OCTO.
10. Members shall ensure they lock their computer or log off the network when not actively using MPDNet.

B. The Electronic Mail (E-mail) System

1. Members shall login to their MPD e-mail account at least once during their tour of duty and shall respond to e-mails within twenty-four (24) hours or during their next assigned tour of duty.
2. Members shall keep their e-mail passwords confidential.
3. Messages sent by and received through members' MPD e-mail accounts are the property of the MPD.
 - a. Members have no property or privacy rights with regard to e-mail messages contained within the MPD e-mail system.
 - b. The content of member e-mail messages may be monitored or retrieved for official investigatory purposes.
 - c. E-mail messages may be subject to release under the Freedom of Information Act (FOIA).
4. E-mail shall not be used to transmit sensitive investigative data. Such information shall be transmitted via appropriate software developed to process investigative information (e.g., WALES, NCIC, and WACIIS).
5. Members shall not intentionally and without authorization from the MPD Chief Technology Officer or authorization from the MPD user intercept, record, read, alter, print, or receive another member's Department e-mail message.

NOTE: Any member who intercepts, records, reads, alters, prints, or receives an individual's private e-mail message without authorization may be subject to civil and criminal penalties.

6. Members may use MPD e-mail for union-related business with the approval of their Commanding Officer.
7. E-mail Retention
 - a. E-mail messages are generally temporary communications of a non-emergency nature; however, depending on the content of the e-mail message, it may be considered a more formal record and should be retained in the appropriate file.

- b. The following are examples of e-mail messages that shall be retained in accordance with MPD policy:
 - (1) Messages that contain potentially discoverable materials which include, but are not limited to, reports, video/audio files, transcripts and photographs. [See GO-SPT-601.02 (Preservation of Potentially Discoverable Materials)].
 - (2) Messages that contain information covered by a litigation hold, information that members independently know is relevant to pending litigation, or members independently know or should reasonably know may be relevant to future litigation. Examples include, but are not limited to, e-mail messages related to:
 - (a) Lawsuits;
 - (b) Claims received from the D.C. Office of Risk Management by the MPD Office of Risk Management;
 - (c) Charges of discrimination filed with the D.C. Office of Human Rights or the Equal Employment Opportunity Commission;
 - (d) Administrative litigation (e.g., grievances);
 - (e) Incidents that involve a police shooting or other serious use of force; and
 - (f) Arrests resulting from a First Amendment activity.

NOTE: E-mail messages to be retained must be preserved in their original electronic format. Paper copies of e-mail messages are not sufficient substitutes. Members may archive e-mail messages through Microsoft Outlook in order to retain e-mail messages indefinitely. Members may contact the MPD-OCTO for assistance with creating e-mail archives.

- 8. Intentional misuse of the e-mail system may subject members to disciplinary or criminal action.
- 9. Members shall not use their e-mail accounts for any of the prohibited activities outlined in Part IV.D of this order.

C. Internet Usage

1. Internet usage by MPDNet users is permitted and encouraged for business purposes in supporting the goals and objectives of MPD and shall be used consistently with the policies set forth in this order.
2. The Internet shall be used for official purposes, including, but not limited to:
 - a. Exchanging e-mail with other MPD members, community members, or other agency partners about public safety and work related issues.
 - b. Performing various forms of work related research.
 - c. Performing word or phrase searches to locate documents.
 - d. Investigating Internet related crime, when assigned or authorized by a Commanding Officer/Director.

D. E-mail and Internet Prohibitions

1. Members **shall not** use MPD e-mail or Internet access to:
 - a. Pursue private commercial business activities or profit-making ventures (e.g., members shall not operate a business using MPD computers and/or MPD provided Internet access).
 - b. Engage in unauthorized fundraising activities of any kind including, but not limited to, the solicitation of funds for personal, financial gain or other non-MPD related benefit.
 - c. Knowingly receive or transmit any files in violation of licensing and/or copyright restrictions.
 - d. Engage in matters directed towards the success or failure of a political party/candidate for partisan political office.
 - e. Access any Internet site resulting in additional costs to the MPD without advance written authorization from his/her Commanding Officer/Director.
 - f. Engage in any prohibited discriminatory conduct which could be construed as contributing to a hostile work environment.
 - g. Obtain, view or send sexually explicit material [except in

those circumstances in which members are authorized as part of their official duties (e.g., to investigate Internet related crimes or other official duties)].

- h. Engage in activities that violate the privacy of other users.
 - i. Engage in conduct meant to purposely or which could misrepresent the identity of the user (except in those circumstances in which members are authorized as part of their official duties).
 - j. Send any material that is obscene or defamatory, or which is intended to annoy, harass or intimidate another person (except in those circumstances in which members are authorized as part of their official duties).
 - k. Create discussion groups without written authorization from the MPD-OCTO.
 - l. Post or release MPD data (e.g., call for service data, arrest data, crime data) without authorization from their Commanding Officer/Director.
 - m. Transmit sensitive or restricted information (e.g., criminal history or juvenile information).
 - n. Engage in activities that would tend to bring discredit on MPD or that violate laws, regulations, or MPD policy or procedure.
- 2. Members shall use caution to prevent MPD computer equipment from contracting viruses or becoming damaged (e.g., by deleting junk email messages without opening them, by using portable storage devices only from known sources).
 - 3. Members who misuse MPD e-mail or Internet services may be subject to disciplinary or criminal penalties.

E. Social Networking

1. Personal Social Networking

- a. Unless previously released by the Department, members shall not post or transmit the following types of information on social network sites:
 - (1) Pictures, depictions, descriptions, or personal information of any victim, witness or suspect;

- (2) Pictures, depictions or description of any crime scene;
 - (3) Information involving previous, current or future investigations.
 - b. In accordance with GO-PER-201.26 (Duties, Responsibilities, and Conduct of Members of the Department), members are reminded that they shall conduct their private and professional lives in such a manner as to avoid bringing discredit upon themselves, MPD, or the District of Columbia.
 - c. Members are cautioned to be mindful of potential safety and security issues they may encounter when identifying themselves as law enforcement officers and/or members of MPD when participating in social networking including, but not limited to:
 - (1) Disclosing home address, phone number(s), and other personally identifiable information;
 - (2) Transmitting or posting pictures or depictions of any MPD issued uniform or any part of a MPD uniform to include personally purchased items which reference or resemble any MPD badge, patch, logo or issued uniform or equipment; or
 - (3) Transmitting or posting pictures or depictions of any issued MPD equipment including vehicles and weapons.
2. Professional Social Networking
 - a. Members who wish to display information on a public networking site in the course of their official duties shall:
 - (1) Ensure their participation on the site is authorized in writing by his/her Commanding Officer.
 - (2) Ensure the content is related to the performance of official duties.
 - (3) Keep the contents of the professional site(s) separate from any personal social networking accounts.
 - b. Members are reminded to be cognizant of the information displayed on social networking sites and to adhere to the applicable restrictions listed in Part IV.E.1 of this order.
3. Notwithstanding any other provision of this policy, a member may post to social media if:

- a. He/she is not on duty;
 - b. He/she expresses a personal viewpoint and does not attribute the viewpoint to the Department;
 - c. He/she does not post any information, images, or material that is either:
 - (1) Confidential or privileged; or
 - (2) Obtained as a result of his or her employment and is part of an on-going criminal investigation or matter; and
 - d. He/she does not violate any District of Columbia law.
- F. Violations of Department policies including, but not limited to GO-PER-201.26 (Duties, Responsibilities, and Conduct of Members of the Department) will result in an administrative investigation that, if sustained, may result in discipline. Nothing in this policy abrogates or alters those prior existing policies.
- G. Notwithstanding any other provision of this policy, a member shall not be prohibited from exercising his or her First Amendment rights, reporting violations or concerns under the District Whistleblower Protection Act (D.C. Official Code § 1-615.51 et seq.) or the Board of Ethics and Government Accountability Establishment and Comprehensive Ethics Reform Amendment Act of 2011 (D.C. Official Code § 1-1161.01 et seq., or making any other legally protected disclosure.

V. PROCEDURES

- A. Helpdesk Services
- 1. Members shall contact the MPD-OCTO Customer Resource Service Center (Helpdesk) at (202) 727-3302 when encountering problems with hardware, software, e-mail, network connection or other MPDNet issues.
 - 2. When a work request cannot be resolved, Helpdesk staff shall escalate the request to the next level of resolution with a twenty-four (24) to forty-eight (48) hour response timeframe, unless it is an urgent or business-critical request in which case there shall be a four (4) to sixteen (16) hour response timeframe.
 - a. Urgent requests include reported problems where the system user cannot perform his/her job functions or any critical problem which has the potential to affect a large segment of system users.

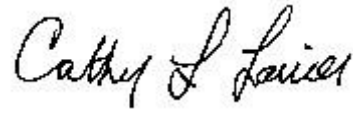
3. Informing the MPD-OCTO when accounts or computers will be used for conducting investigations of Internet-related or other crimes including the usernames of the involved members, the Internet Protocol (IP) addresses of involved computers, and the expected duration of the investigation.

B. MPD-OCTO shall be responsible for:

1. Planning for, reviewing and selecting appropriate hardware and software for use on the MPDNet.
2. Ensuring that there are an adequate number of computers equipped with software at each unit within the MPD including, but not limited to, Internet access.
3. Ensuring MPD hardware and software are used within the vendor/matrix manufacturer recommended environmental parameters (e.g., avoiding excessively high/low temperature, water exposure.)
4. Assigning initial MPDNet user accounts and associated passwords for new users.
5. Accessing computer systems for authorized diagnostic and management purposes from other computer terminals connected to the network.
6. Assisting the Internal Affairs Bureau in obtaining required information from the District of Columbia OCTO for investigations related to member misconduct involving MPDNet hardware or software.
7. Ensuring the Helpdesk provides telephonic support to users twenty-four (24) hours a day, seven (7) days a week, except holidays.
8. Implementing and coordinating MPDNet availability throughout the MPD.
9. Distributing system user manuals and additional information as required.
10. Facilitating the use of specific user accounts and specific computers to conduct investigative activities on the Internet as authorized by the Chief of Police or his/her designee.

VII. CROSS REFERENCES

1. GO-SPT-601.02 (Preservation of Potentially Discoverable Materials)

A handwritten signature in black ink that reads "Cathy L. Lanier". The signature is written in a cursive, flowing style.

Cathy L. Lanier
Chief of Police

CLL:PAB:MOC