PATROL GUIDE

Section: Duties and Responsibilities		Procedure No: 203-28	
DEPARTMENT SOCIAL MEDIA ACCOUNTS AND POLICY			
DATE ISSUED: 04/15/16	DATE EFFECTIVE: 04/15/16	REVISION NUMBER:	PAGE: 1 of 4

PURPOSE To provide procedures for social media account establishment, management, administration, oversight, and guidance for individual use.

DEFINITIONS

SOCIAL MEDIA: A category of internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites, photo and video sharing sites, wikis, blogs, and websites such as Facebook, Instagram, Flickr, YouTube, LinkedIn, Snapchat, and Twitter.

DEPARTMENT SOCIAL MEDIA ACCOUNT: An account established by the Department with a third party provider such as Facebook or Twitter.

HOSTING PRIVILEGES: The privilege of hosting an official NYPD social media account. The account host is responsible for all content appearing on the account.

POSTING PRIVILEGES: The privilege of posting to an official NYPD social media account such as a Facebook page or Twitter account.

PROCEDURE When commands/units wish to establish a Department social media account:

REQUESTING COMMAND/UNIT

1. Forward request on **Typed Letterhead** to Deputy Commissioner, Strategic Communications (DCSC).
   a. Include list of command/unit members who will be granted hosting/posting privileges.

NOTE *In general, only commanding officers, bureau chiefs and deputy commissioners are authorized to establish a Department social media account. Exceptions will be made on a case-by-case basis, and only with the approval of DCSC. Commands are prohibited from hosting their own individual sites without approval of DCSC. Unauthorized accounts will be ordered closed.*

DEPUTY COMMISSIONER, STRATEGIC COMMUNICATIONS

2. Review request and endorse (approved/disapproved):
   a. If approved:
      (1) Coordinate with the Information Technology Bureau (ITB) to ensure that the proper protocols are followed regarding the establishment of a new account
      (2) Provide Department Social Media training for members requesting hosting/posting privileges
      (3) Upon completion of training, file original endorsed request and forward a copy to originating command indicating that new account has been established, and the list of members that have completed training and are authorized for hosting/posting privileges.
   b. If disapproved, file original endorsed request and forward a copy to originating command indicating reason.

NOTE *DCSC is the primary liaison to commands maintaining or establishing Department social media accounts, and is available to provide training, guidance and assistance. Technical questions concerning mobile device access, browser compatibility, etc., should be referred to ITB. During large scale or emergency incidents, members will be guided by Operations Order 9, series 2016, "Social Media Plan: Emergency Incidents."*

INFORMATION TECHNOLOGY BUREAU

3. Provide DCSC with any needed assistance in the creation and establishment of approved social media accounts.
   a. Include guidelines on appropriate passwords required to be used by commands/units.

WHEN A DEPARTMENT SOCIAL MEDIA ACCOUNT HAS BEEN COMPROMISED

COMMANDING OFFICER/ SUPERVISORY MEMBER

4. Notify the following upon becoming aware that a Department social media account has been compromised (i.e., personal identifying data posted, hacked account, etc.):
   a. Deputy Commissioner, Strategic Communications
   b. Deputy Commissioner, Public Information
   c. Information Technology Bureau Wheel
   d. Intelligence Bureau, Operations Unit (when a threat is made against a member of service).

DEPUTY COMMISSIONER, STRATEGIC COMMUNICATIONS

5. Confer with ITB and hosting company concerned (e.g., Twitter, Facebook, etc.) to determine corrective actions necessary for safeguarding account status.
6. Advise member concerned regarding necessary actions.

NOTE *In instances where a threat is made against a member of the service, DCSC will confer with the Intelligence Bureau/investigative unit concerned prior to determining actions regarding account status. For instance, investigators may request that a compromised account remain active to allow time to obtain information to enhance the investigation. In all cases, P.G. 212-31, "Threats Against Members of the Service" will be followed.*

Upon receiving a request for information from representatives of the media, or when responding to newsworthy incidents, members of the service will comply with the provisions of P.G. 212-77, "Release of Information to News Media." For incidents involving members of the media, members of the service are reminded to comply with the provisions of P.G. 212-49, "Incidents Involving Media Representatives."

ADDITIONAL DATA

DEPARTMENT POLICY

No Department social media account is to be established except that which has been authorized by endorsement of the Deputy Commissioner, Strategic Communications. Members of service granted hosting privileges will be required to attend training provided by DCSC. Commanders/Account Hosts may designate one or more members of their command to post content on behalf of the command; DCSC will be advised and updated of any/all designees granted posting privileges. Only DCSC personnel, a host, or his/her designee, if authorized and trained, may post content to a NYPD social media site.

ADDITIONAL DATA (continued)

In accordance with P.G. 203-10, "Public Contact – Prohibited Conduct," members of the service are prohibited from using Department or command identifiers as part of a privately held social media account moniker (e.g., @nypd_johndoe, @053Pct_janedoe, etc.).

PERSONAL USE OF SOCIAL MEDIA BY MEMBERS OF THE SERVICE

Members of the service are to be cognizant of their personal use of social media sites. Any activities or statements made on social media sites are done so in an online domain where users have no reasonable expectation of privacy. Even if a member of the service has created "private" or "limited access" accounts or has customized "privacy settings," any statements, photographs, video clips or information which are sent over the internet may still be viewed and disseminated by third parties, even after the content has been edited or deleted by the user. When assessing actions that may violate this Order, be guided by common sense standards of reasonableness. Violations of this Order may subject members of the service to disciplinary action. All provisions of P.G. 203-10, "Public Contact - Prohibited Conduct" continue to apply to the use of social media.

Members of the service utilizing personal social media sites are to exercise good judgment and demonstrate the same degree of professionalism expected of them while performing their official duties. Members of the service should be aware that activities on personal social media sites may be used against them to undermine their credibility as members of the Department, interfere with official police business, compromise ongoing investigations and affect their employment status with the Department. Furthermore, information (including digital images) released on social media may endanger the safety of members of the service and/or their family members. Members of the service are urged not to disclose or allude to their status as a member of the Department. Divulging identifying information on social media sites may endanger officer safety and may limit a member of the service's eligibility for certain assignments. Members of the service who serve or seek to serve in an undercover capacity or work in highly sensitive assignments are particularly at risk. Because of the potential risks associated with the disclosure of one's status as a member of the Department, members of the service are prohibited from revealing Department affiliations of other individuals (e.g., partners, co-workers, supervisors, etc.) without the express consent of that individual. These restrictions include, and are not limited to, the individual posting, "tagging" and/or "sharing" pictures of other members of the service. Members of the service are prohibited from posting photographs of themselves in uniform and/or displaying official identification, patches or badges, marked/unmarked vehicles on internet sites without authorization from the Department. These prohibitions will not apply to photographs taken at official Department ceremonies (e.g., promotions, awards, medal/citations, etc.). Members of the service are prohibited from posting on the internet nonpublic items (e.g., witness statements, crime scene photographs, videos, etc.) that were gained as a result of their position with the Department.

Members of the service are prohibited from knowingly engaging in any type of social media contact (e.g., "friending," "following," etc.) with a suspect, witness, or crime victim if that officer was either involved in the incident, or the officer became acquainted with that victim or witness during or because of the incident and the matter is under investigation or pending in a criminal court. Further, members of the service will not knowingly engage in social media contact about a matter under investigation or pending in criminal court with a lawyer who is working on that matter.

ADDITIONAL DATA (continued)

Members of the service are prohibited from engaging in any type of social media contact (e.g., "friending," "following," etc.) with minors they interact with in the course of their employment with the Department. Such communications may be deemed inappropriate and create an appearance of impropriety. These restrictions do not bar such communication with relatives of the member of the service. This policy applies to both official use of social media and personal use of social media by members of the service. All members of the service are reminded that they are strictly accountable for their conduct at all times, whether on or off duty, inside or outside of New York City.

RELATED PROCEDURES

Department Confidentiality Policy (P.G. 203-22)
Information Concerning Official Business of Department (P.G. 212-76)
Department Computer Systems (P.G. 219-14)
Department Computer Use Policy and Monitoring Notice (A.G. 325-35)
Performance on Duty – Prohibited Conduct (P.G. 203-06)
Public Contact – Prohibited Conduct (P.G. 203-10)
Public Contact – General (P.G. 203-09)
Threats Against Members of the Service (P.G. 212-31)
Release of Information to News Media (P.G. 212-77)
Incidents Involving Media Representatives (P.G. 212-49)
Use of Social Networks For Investigative Purposes – General Procedure (Operations Order 34, series 2012)
Social Media Plan: Emergency Incidents (Operations Order 9, series 2016)