SOCIAL MEDIA

DRAFT

POLICY & PROCEDURE NO. **X.XX**	ISSUE DATE: _____
	EFFECTIVE DATE: _____
MASSACHUSETTS POLICE ACCREDITATION STANDARDS REFERENCED: **None**	REVISION DATE: _____

I. GENERAL CONSIDERATIONS AND GUIDELINES

Social media sites, chat rooms, forums, and comment sections allow interactions between some people who would never have been able to communicate prior to their development. People with differing backgrounds, levels of experience and geographical regions can now share ideas, thoughts and practices; long lost friendships and acquaintances may be rediscovered; and news, methods and procedures may be shared. Electronic media has made many things, previously thought impossible, possible.

However, such media has also created previously unforeseen hazards. The topics of locker rooms, roll-call chatter and verbal horsing around, removed from those venues and publicly posted has ended careers, damaged reputations, and complicated or damaged otherwise sound prosecutions.

Although the advent of social media is relatively new to law enforcement, little have the hazards and pitfalls changed. To paper and the spoken word has been added electronic media, with a breadth and speed which far exceeds either.

The internet holds no secrets. Social media sites and forums are public and chat rooms have leaks. Never assume privacy or security on these sites. Always assume that what you post will be seen publicly. What is posted or e-mailed today may live

forever, dredged from the depths of some nameless server by some search term on some search engine.

The topics and antics of the locker room and roll-call rooms may be kept in their proper context in those places – a joke; a prank; comradeship. The same in public, out of its element and out of context, damages reputations, destroys careers and impeaches witnesses.

II. POLICY

It is the policy of this department that:

1. Employees shall not, intentionally or unintentionally, bring discredit upon themselves or this agency through electronic devices and/or social media.
2. Employees shall not use electronic devices or social media to violate the policies, procedures, rules, or regulations of this agency.
3. Employees shall not disclose unauthorized or confidential information and/or materials using electronic devices or social media.

III. DEFINITIONS

A. ***Chat:*** Digital text communications between two or more persons. The text is generally posted in the order sent for all of the participants to read.

B. ***Electronic Devices:*** Cellular telephones, Ipads, digital cameras, mobile computers, mini-computers, desktop computers, and other devices used to store or transfer data, live audio or video, location or other information.

C. ***Forum:*** Discussion areas on web sites where people can post messages and make comments. Some forums allow users to upload images, audio, video and other files.

D. ***Friends:*** On social networking sites, friends are individuals or organizations that you authorize to view the materials that you and others post to your site, and may allow you to view the materials posted on their site.

E. ***Peer-to-Peer:*** The connection of two or more individuals or organizations through a network. Peer-to-peer is often associated with file sharing.

F. ***Profiles:*** Information, images, audio, and/or video that a person or organization provides about themselves on a social networking site.

G. ***Public Domain:*** Materials or access available to the public without any special permission or access.

H. ***Social Media:*** A platform for individuals and organizations to interact and/or share information and electronic content. Examples include Facebook, LinkedIn and Twitter.

I. ***Social Networking:*** A platform for individuals and organizations to communicate and share information with others at varying levels of their social network. Some well-known social networking sites are: Facebook, Twitter, My Space and LinkedIn. In addition, various "police" sites are now available for officers and potentially others to post information and video.

IV. PROCEDURES

A. *Department Authorized Social Media*:

1. Authorization: No employee shall create, maintain, or contribute to any social media site representing the police department or identifying themselves as a member of this department unless authorized by **[IDENTIFY – CHIEF, OTHER OFFICIAL, ETC]**.
2. Sites: Specific authorization must be obtained for each site or profile.
3. Profile: Official department profiles or the department profiles of individual employees reflect upon the agency and staff as a whole. Official sites must be presented in a professional and honorable manner which will not discredit the department, its mission, or employees.
4. Content
    a. Site content may be reviewed for compliance with this policy. Content which, in the opinion of the Chief of Police **[or –IDENTIFY OTHERS]**, is not in compliance with department policy or is inappropriate, may be ordered removed.
    b. Personnel Information:
        1) Official Personal Information: Official sites may include official information regarding the agency and employees. Official information includes, but is not limited to:
            a) Date of hire;
            b) Years of service;
            c) Previous law enforcement employment;
            d) Previous military service;

e) Present military status;

f) Present department assignment;

g) Rank;

h) Specialty training

i) Performance awards and achievements;

j) Educational achievements; and

k) Any public record information.

2) General Personal Information: Individual employees may authorize their general personal information to be presented. General personal information includes, but is not limited to:

a) Home city or town;

b) Present city or town of residence;

c) Age;

d) Present marital status, children;

e) Present military assignment;

3) Specific information about employees and their family members shall not be posted. Specific personal information includes, but is not limited to:

a) Dates of birth of employees or family members;

b) Addresses of employees or family members;

c) Personal telephone numbers, e-mail addresses, etc.

4) No personal information other than official personal information may be posted about any employee against that employee's wishes.

c. Contact Information: Only official department contact information shall be posted.

d. Images:

1) Official department images are authorized to be published on official department sites. Official department images include, but are not limited to:

a) Town/City seal;

b) Department patch;

c) Department badges;

d) Department personnel: On duty photos and images of department personnel.

NOTE: Photos of employees working in an under cover or confidential assignments are considered confidential.

e) Department buildings;

f) Department vehicles;

2) Department controlled images remain the property of the department. Such images **[SHALL NOT BE POSTED OR MAY BE POSTED IF AUTHORIZED BY – IDENTIFY]**. Department controlled images include, but are not limited to:

a) Photos and/or video taken while on duty;

b) Photos and/or video taken in areas not open to the public;

c) Photos and/or video of crime scenes and/or victims.

e. Confidentiality:

1) Information considered confidential shall not be posted unless authorized by **[IDENTIFY – CHIEF, OTHER OFFICIAL, ETC]**.

2) Nothing posted on any social networking site can ever be considered confidential.

f. Opinion: Statements and content should represent those of the agency and not personal opinions.

1) Individual writers may state opinion when promoting department services, such as relating personal experiences when receiving such services.

2) Individual writers may state opinion when writing blogs or articles, provided an opinion disclaimer is used.

5. Personal Messaging:

a. Employees engaged in personal messaging must keep such messaging professional at all times.

b. Be mindful of and guard against messages which may be considered inappropriate.

c. Be cautious when communicating outside of public areas with children and persons with whom personal involvement would be considered inappropriate.

d. Avoid messages which include disbursing personal, C.O.R.I., investigative or other confidential information. Such messaging cannot be considered confidential or secure. Sensitive messages should be communicated through more secure means.

6. Prohibited Content: The following content is prohibited.

a. Discrimination (race, sex, sexual orientation, religion, national origin, etc.);

b. Obscene materials;

c. Harassment, including sexual harassment;

d. Infringement of copyrighted material;

e. Conduct of personal business, outside business, or promotion of private businesses.

f. Expression of support of any political party or candidates.

B. *Department Sanctioned Social Media for Investigations*

1. Authorization:

a. No employee shall create, maintain, or contribute to any social media site for investigative purposes unless authorized by **[IDENTIFY – CHIEF, OTHER OFFICIAL, ETC]**.

b. Sites: Specific authorization must be obtained for each site or profile.

2. Equipment:

a. Only department equipment (computers, cellular phones, etc.) may be used. Employees shall not use personal equipment or devices when visiting pornographic or sexual sites for investigations.

b. Such equipment must be set up so as to have no on-line identifiers to the department's network or otherwise be identifiable to law enforcement.

c. Equipment should not be connected to the department network, if possible.

3. False Identities and Profiles:

a. The use of false identities for investigative purposes must be authorized by **[IDENTIFY – CHIEF, OTHER OFFICIAL, ETC]**.

b. The details of false identities and profiles, must be:

1) Documented;

2) Approved by the investigations supervisor prior to use; and

3) Treated as confidential.

c. Terms of Service Agreements: Most social networking sites require that users agree to abide by certain terms of service in order to use their site. Employees are responsible for understanding the terms of service for each site used. Many such sites prohibit the use of false names and posting of false information on their site. Employees must be aware that if their true identity is discovered by a site host, their account may be disabled and the investigation may be compromised.

4. Review of Conduct: Employees conducting on-line undercover investigations will meet periodically with **[INVESTIGATIONS COMMANDER OR IDENTIFY]** to review the conduct of the investigation. The purpose of the review is to ensure that the investigator is following agency policy and procedures and to protect the employee from later claims of secrecy and investigational misconduct.

C. *Personal Social Media*

1. Generally:

a. The department will generally limit its inquiring into an employee's off-duty conduct to situations impacting or reflecting upon the department or affecting the employee's ability or fitness for duty.[1]

b. The department has a legitimate interest in preserving the public's trust and respect. An employee's off-duty personal relationships and conduct must not bring discredit to the employee or department, impact on the Department's operation, affect the employees; ability to perform his or her job or result in poor job performance.[2]

c. In social networking, chat, blog and news comment sites, an employee's status as a police employee may become known either by the employee making such an affiliation known, by others making the employee's affiliation known, by disclosure from the site's host, discovery in a civil or criminal proceeding, or other methods. Employees must be aware that inappropriate comments, files, images and other materials posted by them or affiliated with their on-line profile may damage their fitness to serve in the eyes of the public.

2. Conduct Unbecoming

a. Employees do not sever their relationship with the department at the end of their shift. An officer's off-duty conduct, especially where there is some nexus or connection to the department where the officer's status as a police officer is or becomes known, may reflect unfavorably on both the officer and department.

b. Although the disciplinary charge of "Conduct Unbecoming" does not apply to non-sworn employees, the ties between an employee's off duty conduct and their fitness for employment by the agency still do.

c. Employees must be aware that prohibited conduct, on or off duty, and the disciplinary offense of "conduct unbecoming" applies to social networking, blogging, chat, and other on-line activity as well.

d. Do not cross the line between funny and inappropriate.

e. Employees must be mindful that violation of department rules, regulations, policies and procedures apply to employees' on-line activities.

3. Identification of Social Media Activity for Internal Investigations. During the course of a departmental investigation, employees may:

a. Be ordered to provide the department, or its designated investigator, a listing of and access (e.g., password, user name, etc.) to any social media and social networking platforms in which they participate or maintain.

b. Be ordered to complete an affidavit attesting to all of the social medial and social networking platforms in which they participate or maintain.

4. Investigative Activities: No employee may conduct any department related investigative activity using a personal social networking account.

5. **[OPTIONAL]** Display of Department Information and Property:

a. Text, images, photographs or other reproductions of the **[CITY/TOWN]** or police department logo's, seals, patches, letterhead, uniforms or other insignia affiliated with this department is **[AUTHORIZED/PROHIBITED]**.

b. Text, images, photographs, and video of buildings, equipment, vehicles and scenes affiliated with this department and not within the public domain is **[AUTHORIZED/PROHIBITED]**.

c. Text, images, photographs, and video of crime scenes and investigations, past and present and not within the public domain is **[AUTHORIZED/ PROHIBITED - CONDITIONS]**.

6. **[OPTIONAL]** Self-Identification as a Department Employee

a. Employees **[MAY OR SHALL NOT]** identify themselves as department employees on any social networking site or over the Internet except as part of their official duties.

b. Employees who appear in uniform or otherwise indirectly disclose their affiliation with the department have identified themselves department employees.

7. Prohibited Without Specific Authorization: Unless specifically authorized by **[IDENTIFY – CHIEF, OTHER OFFICIAL, ETC]** the following activities are prohibited on any employee's personal social networking sites:

   a. **[OPTIONAL]** References to oneself as a department employee;

   b. Identifying other employees as members of this department;

   c. **[OPTIONAL]** References to the employee's department rank and/or title, including in on-line identity and profiles;

   d. **[OPTIONAL]** Photos, video, or other depictions of employees in uniform.

8. Prohibited: The following activities are prohibited on an employee's personal social networking sites:

   a. Postings or material that detracts from the department's mission;

   b. Disclosing any confidential law enforcement missions (search warrants, warrant sweeps, investigations, etc.)

   c. Criminal Offender Record Information (C.O.R.I) or other protected information.

   d. Identifying employees of other law enforcement agencies (local, state, or federal) as law enforcement employees;

   e. Identifying informants, victims, suspects, or witnesses to any crime or investigation to which this department is affiliated unless the information is already within the public domain;

   f. Sexually graphic and explicit materials of any kind including nude or sexually suggestive images of the employee;

   g. Disparaging remarks or materials targeting **[CITY/TOWN]** or department employees or their family members.

   h. Disparaging remarks or materials targeting persons, organizations, or businesses which the employee has dealt with due to department employment.

i. Harassment, including sexual harassment;

j. Criminal behavior;

k. Threats against the President of the United States;

l. Displaying images of other employees without their permission.

9. Strongly Discouraged: The following may be within an employee's speech rights, but could pose a risk of conduct unbecoming. Again, an employee's public posting could damage an employee's fitness to serve as a law enforcement employee. Embarrassing or inappropriate material which is posted may be publicly available forever.

   a. **[OPTIONAL]** Identifying oneself as a department employee.

   b. Profanity;

   c. Rude, discourteous, or discouraging remarks;

   d. Comments regarding personal drunkenness or heavy alcohol use.

[1] 4.0 of the department Rules and Regulations.

[2] 4.0 of the department Rules and Regulations.