

Neptune City Police Department  GENERAL ORDER		DATE: May 23, 2016	NUMBER: GO-02-2016
		SUBJECT: Electronic Messaging and Internet	
REFERENCE: 	RESCINDS: 	DISTRIBUTION: 	

I. PURPOSE

It is the purpose of this policy to provide Neptune City Police Officers with guidance on the proper use of personal computers and related electronic messaging systems utilized in this agency for purposes of disseminating electronic mail, utilizing services of the Internet and related electronic message transmission, recording and storage devices.

II. POLICY

The availability and use of the personal computer within the work environment have provided many opportunities for enhancement of productivity and effectiveness. These technologies also entail the opportunity for rapid transfer and broad distribution of sensitive information that can also have damaging effects on this agency, its members, and the public if not managed properly. Therefore, it is the policy of this agency that all members abide by the guidelines set forth herein when using personal computers and the services of both internal and external databases and information exchange networks, and where applicable, voice mail, mobile digital terminals, and related electronic messaging devices.

III. DEFINITIONS

Electronic Messaging Device (EMD): For purposes of this policy, electronic messaging devices include personal computers, electronic mail systems, voice mail systems, paging systems, electronic bulletin boards and Internet services, mobile digital terminals, and facsimile transmissions.

System Administrator: For purposes of this policy, the member of this agency designated with responsibility for managing all aspects of electronic messaging through individual computers and computer networks within this agency.

Personal Computer: Any agency or personally owned computer that provide access to the agency or agency personnel. This includes both on and off duty usage.

IV. PROCEDURES

A. General

1. The following procedures apply to all media which are:
 - a. Accessed on or from departmental premises;
 - b. Accessed using department computer equipment or department paid access methods;
 - c. Communications that make reference to the department in a manner; and/or
 - d. Used in a manner that identifies the employee with the department.
 - e. The Neptune City Police Department electronic mail (email system) is; yourname@neptunecitypolice.org or the assigned email from ncpd***@optonline.net to certain officers.
2. Transmission of electronic messages and information on communications media provided for employees of the Neptune City Police Department shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence, or verbal communication.
3. The Neptune City Police Department encourages authorized and trained personnel with access to EMDs to utilize these devices whenever necessary. However, use of any of these devices is a privilege that is subject to revocation.

EMDs and their contents—with the exception of personally owned software authorized for installation on agency computers—are the property of this agency and intended for use in conducting official business with limited exceptions noted elsewhere in this policy.

4. Members are advised that they do not maintain any right to privacy in EMD equipment or its contents, to include personally owned software.
 - a. This agency will monitor information contained in EMDs and may require members to provide passwords to files that have been encrypted or password protected.

- b. The agency shall access, for quality control purposes and/or for violations of this policy, electronic and voice transmissions of members conducting business of this agency.
- 5. Computer repairs shall be made by the Neptune City Police Department's authorized and approved sources.
- 6. Accessing or transmitting materials (other than that required for police business) that involves the use of obscene language, images, jokes, sexually explicit materials, or messages that disparage any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material.
- 7. Confidential, proprietary, or sensitive information may be disseminated (or made available through shared directories or networked systems) only to individuals with a need and a right to know and when there is sufficient assurance that appropriate security of such information will be maintained. Such information includes but is not limited to the following:
 - a. Transmittal of personnel information, such as salary, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records, or related employee information.
 - b. Criminal history information and confidential informant master files, identification files, or related information.
 - c. Intelligence files and information containing sensitive tactical and undercover information.
- 8. Employees may not attempt to read or "hack" into other systems or logins; "crack" passwords; breach computer or network security measure; or monitor electronic filings or communications of other employees or third part except by explicit direction of departmental authorities.
- 9. No e-mail or other electronic communications may be sent that attempts to hide the identity of the sender or represents the sender as someone else or someone from another agency.
- 10. Media may not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.
- 11. Employees may not copy, retrieve, modify, or forward copyrighted materials except as permitted by the copyright owner or except for a single copy for reference use only.
- 12. No member shall access or allow others to access any file or database unless that person has a need and a right to such information.

Additionally, personal identification and access codes shall not be revealed to any unauthorized source.

13. An EMD is designed and intended to conduct business of this agency and is restricted to that purpose. Installation of or access to software for purely entertainment purposes is prohibited. Exceptions to business use include the following:
 - a. Infrequent personal use of these devices may be permissible if limited in scope and frequency, if in conformance with other elements of this policy, and if not connected with a profit-making business enterprise or the promotion of any product, service, or cause that has not received prior approval of this agency.
 - b. Personnel may make off-duty personal use of agency computers for professional and career development purposes when in keeping with other provisions of this policy and with prior knowledge of an appropriate supervisor.

B. Importing/Downloading Information and Software

1. Members shall not download or install on their personal computer or network terminal any file (including sound and video files and files attached to e-mail messages), software, or other materials from the Internet or other external sources without taking prescribed steps to preclude infection by computer viruses.
 - a. Material shall be downloaded to floppy drives and scanned for viruses prior to being entered into any personal or shared system.
 - b. In no case shall external materials or applications be downloaded directly to any shared (network) drive. When in doubt, members shall consult the system manager for guidance.
2. Members shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.
 - a. Any software for which proof of licensing (original disks, original manuals and/or license) cannot be provided is subject to removal by authorized agency personnel.
 - b. Privately owned software may be loaded on agency computers if approved by the system administrator.
 - c. Privately owned software may be removed if it conflicts with departmental hardware or software, interferes with the ability of other members to access or utilize the EMD, or occupies excessive storage space needed by the agency.

3. Members shall observe copyright restrictions of any documents, images, or sounds sent through or stored on electronic mail.
4. Any hardware enhancements or additions to agency-owned equipment must be approved and authorized by the system administrator. The system administrator is responsible for determining proper installation procedures.
5. Members shall not permit unauthorized persons to use this agency's electronic mail system.
6. To avoid breaches of security, members shall log off any personal computer that has access to the agency's computer network, electronic mail system, the Internet, or sensitive information whenever they leave their workstation.

This policy is developed by the Neptune City Police Department for internal use only, and does not enlarge an officer's civil or criminal liability in any way. This policy should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this policy can only be the basis of a complaint by this department, and then only in an administrative disciplinary setting.

All employees will sign the verification form placed at the Neptune City Dispatch Desk, acknowledging receipt, review and understanding of GO 02-2016.

By order of the Director of Public Safety



Edward D. Kirschenbaum, Sr.
Neptune City Police Department

EDK: syh

C:
Mayor Robert Brown
Councilman Joseph Zajack
Borough Administrator Mary Sapp

Neptune City Police Department  GENERAL ORDER		DATE: May 23, 2016	NUMBER: GO-05-2016
		SUBJECT: Social Media Use	
REFERENCE:	RESCINDS:	DISTRIBUTION:	

I. PURPOSE

The Neptune City Police Department endorses the secure use of social media to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. This policy establishes this department's position on the utility and management of social media and provides guidance on its management, administration, and oversight. This policy is not meant to address one particular form of social media, rather social media in general, as advances in technology will occur and new tools will emerge.

II. POLICY

Social media provides a new and potentially valuable means of assisting the department and its personnel in meeting community outreach, problem-solving, investigative, crime prevention, and related objectives. This policy identifies potential uses that may be explored or expanded upon as deemed reasonable by administrative and supervisory personnel. The department also recognizes the role that these tools play in the personal lives of some department personnel. The personal use of social media can have bearing on departmental personnel in their official capacity. As such, this policy provides information of a precautionary nature as well as prohibitions on the use of social media by department personnel.

III. DEFINITIONS

Blog: A self-published diary or commentary on a particular topic that may allow visitors to post responses, reactions, or comments. The term is short for "Web log."

Page: The specific portion of a social media website where content is displayed, and managed by an individual or individuals with administrator rights.

Post: Content an individual shares on a social media site or the act of publishing content on a site.

Profile: Information that a user provides about himself or herself on a social networking site.

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 (Facebook,), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

Social Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

Speech: Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

Web 2.0: The second generation of the World Wide Web focused on shareable, user-generated content, rather than static web pages. Some use this term interchangeably with social media.

Wiki: Web page(s) that can be edited collaboratively.

IV. ON-THE-JOB USE

A. Department-Sanctioned Presence

1. Determine strategy

- a. Where possible, each social media page shall include an introductory statement that clearly specifies the purpose and scope of the agency's presence on the website.
- b. Where possible, the page(s) should link to the department's official website.
- c. Social media page(s) shall be designed for the target audience(s) such as youth or potential police recruits.

2. Procedures

- a. All department social media sites or pages shall be approved by the chief executive or his or her designee and shall be administered by the departmental information services section or as otherwise determined.
- b. Where possible, social media pages shall clearly indicate they are maintained by the department and shall have department contact information prominently displayed.
- c. Social media content shall adhere to applicable laws, regulations, and policies, including all information technology and records management policies.
 1. Content is subject to public records laws. Relevant records retention schedules apply to social media content.
 2. Content must be managed, stored, and retrieved to comply with open records laws and e-discovery laws and policies.

- d. Where possible, social media pages should state that the opinions expressed by visitors to the page(s) do not reflect the opinions of the department.
 1. Pages shall clearly indicate that posted comments will be monitored and that the department reserves the right to remove obscenities, off-topic comments, and personal attacks.
 2. Pages shall clearly indicate that any content posted or submitted for posting is subject to public disclosure.

3. Department-Sanctioned Use

- a. Department personnel representing the department via social media outlets shall do the following:
 1. Conduct themselves at all times as representatives of the department and, accordingly, shall adhere to all department standards of conduct and observe conventionally accepted protocols and proper decorum.
 2. Identify themselves as a member of the department.
 3. Not make statements about the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions, nor post, transmit, or otherwise disseminate confidential information, including photographs or videos, related to department training, activities, or work-related assignments without express written permission.
 4. Not conduct political activities or private business.
- b. The use of department computers by department personnel to access social media is prohibited without authorization.
- c. Department personnel use of personally owned devices to manage the department's social media activities or in the course of official duties is prohibited without express written permission.
- d. Employees shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.

B. Potential Uses

1. Social media is a valuable investigative tool when seeking evidence or information about
 - a. missing persons;
 - b. wanted persons;
 - c. gang participation;
 - d. crimes perpetrated online (i.e., cyberbullying, cyberstalking); and
 - e. photos or videos of a crime posted by a participant or observer.
2. Social media can be used for community outreach and engagement by
 - a. providing crime prevention tips;
 - b. offering online-reporting opportunities;

- c. sharing crime maps and data; and
 - d. Soliciting tips about unsolved crimes (i.e., Crime stoppers, text-a-tip).
- 3. Social media can be used to make time-sensitive notifications related to
 - a. road closures,
 - b. special events,
 - c. weather emergencies, and
 - d. missing or endangered persons.
- 4. Persons seeking employment and volunteer positions use the Internet to search for opportunities; and social media can be a valuable recruitment mechanism.
- 5. This department has an obligation to include Internet-based content when conducting background investigations of job candidates.
- 6. Searches should be conducted by a non-decision maker. Information pertaining to protected classes shall be filtered out prior to sharing any information found online with decision makers.
- 7. Persons authorized to search Internet-based content should be deemed as holding a sensitive position.

Search methods shall not involve techniques that are a violation of Existing law.

- 8. Vetting techniques shall be applied uniformly to all candidates.
- 9. Every effort must be made to validate Internet-based information considered during the hiring process.

V. PERSONAL USE

A. Precautions and Prohibitions

Barring state law or binding employment contracts to the contrary, department personnel shall abide by the following when using social media.

- 1. Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair working relationships of this department for which loyalty and confidentiality are important, impede the performance of duties, impair discipline and harmony among coworkers, or negatively affect the public perception of the department.
- 2. As public employees, department personnel are cautioned that speech on- or off-duty, made pursuant to their official duties—that is, that owes its

existence to the employee's professional duties and responsibilities—is not protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the department. Department personnel should assume that their speech and related activity on social media sites will reflect upon their office and this department.

3. Department personnel shall not post, transmit, or otherwise disseminate any information to which they have access as a result of their employment without written permission from the chief executive or his or her designee.
4. For safety and security reasons, department personnel are cautioned not to disclose their employment with this department nor shall they post information pertaining to any other member of the department without their permission. As such, department personnel are cautioned not to do the following:
 - a. Display department logos, uniforms, or similar identifying items on personal web pages.
 - b. Post personal photographs or provide similar means of personal recognition that may cause them to be identified as a police officer of this department. Officers who are, or who may reasonably be expected to work in undercover operations, shall not post any form of visual or personal identification.
5. When using social media, department personnel should be mindful that their speech becomes part of the worldwide electronic domain. Therefore, adherence to the department's code of conduct is required in the personal use of social media. In particular, department personnel are prohibited from the following:
 - a. Speech containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals.
 - b. Speech involving themselves or other department personnel reflecting behavior that would reasonably be considered reckless or irresponsible.
6. Engaging in prohibited speech noted herein, may provide grounds for undermining or impeaching an officer's testimony in criminal proceedings. Department personnel thus sanctioned are subject to discipline up to and including termination of office.

Department personnel may not divulge information gained by reason of their authority; make any statements, speeches, appearances, and endorsements; or publish materials that could reasonably be considered to represent the views or positions of this department without express authorization.

7. Department personnel should be aware that they may be subject to civil litigation for

- a. publishing or posting false information that harms the reputation of another person, group, or organization (defamation);
 - b. publishing or posting private facts and personal information about someone without their permission that has not been previously revealed to the public, is not of legitimate public concern, and would be offensive to a reasonable person;
 - c. using someone else's name, likeness, or other personal attributes without that person's permission for an exploitative purpose; or
 - d. publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.
8. Department personnel should be aware that privacy settings and social media sites are constantly in flux, and they should never assume that personal information posted on such sites is protected.

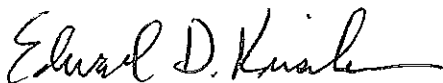
Department personnel should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the department at any time without prior notice.

9. Reporting violations—Any employee becoming aware of or having knowledge of a posting or of any website or web page in violation of the provision of this policy shall notify his or her supervisor immediately for follow-up action.

This policy is developed by the Neptune City Police Department for internal use only, and does not enlarge an officer's civil or criminal liability in any way. This policy should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this policy can only be the basis of a complaint by this department, and then only in an administrative disciplinary setting.

All employees will sign the verification form placed at the Neptune City Dispatch Desk, acknowledging receipt, review and understanding of GO 05-2016.

By order of the Director of Public Safety



Edward D. Kirschenbaum, Sr.
Neptune City Police Department

EDK: syh

C:
Mayor Robert Brown
Councilman Joseph Zajack
Borough Administrator Mary Sapp