



University of Pennsylvania Police Department 4040 Chestnut Street, Philadelphia, Pa 19104		 
Directive: 105	Subject: Use of Electronic Resources, Social Media, and Networking	Effective Date: 11/18/2014
Order of: Gary Williams, Chief of Police		Amended Date: 08/01/2023

I. Purpose

The purpose of this directive is to establish guidelines for the proper use of University of Pennsylvania owned electronic resources and the employ of social media and social networking by University of Pennsylvania Police Department (UPPD) personnel.

Social media may be potentially valuable means of assisting the department with community relations, problem solving, investigations and crime prevention. Social media also plays a significant role in the personal lives of numerous department employees. However, it must be formally and universally recognized that the personal use of social media has the potential to impact the department as a whole, as well as individual members serving 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 UPPD personnel.

As members of the University of Pennsylvania Police Department, employees are embodiments of the mission of the department. It is, thus, essential that each member accept his or her role as an ambassador of the department. In doing so, each member must strive to maintain public trust and confidence, not only in their professional capacity, but also in their personal and on-line activities. Moreover, as police personnel are necessarily held to a higher standard than general members of the public, the on-line activities of employees of the University of Pennsylvania Police Department shall reflect such professional expectations and standards.

II. Policy

It is the policy of the UPPD that all members abide by the guidelines set forth herein when using personal or University owned computers and the services of both internal and external databases, e-mail, information exchange network, voice mail, mobile data terminals or other related electronic messaging devices whether on or off duty. UPPD personnel shall be guided by the University of Pennsylvania Policy on Acceptable Use of Electronic Resources at the following link:
<http://www.upenn.edu/computing/policy/aup.html> .

The General Standards for the Acceptable Use of Computer Resources require:

- Responsible behavior with respect to the electronic information environment at all times;
- Behavior consistent with the mission of the University and with authorized activities of the University or members of the University community;
- Respect for the principles of open expression;
- Compliance with all applicable laws, regulations, and University policies;
- Truthfulness and honesty in personal and computer identification;
- Respect for the rights and property of others, including intellectual property rights;
- Behavior consistent with the privacy and integrity of electronic networks, electronic data and information, and electronic infrastructure and systems; and
- Respect for the value and intended use of human and electronic resources.

The University of Pennsylvania Police Department endorses the secure use of social media to enhance morale, communication, collaboration, and information exchange and foster productivity. This policy establishes the department's position on the utility and management of social media and provides guidance on its use by UPPD personnel. In so doing, this policy sets forth expectations of police department employees with respect to their use of social media and social networking, and the direct effect such use has upon the reputation, perception and interests of the University of Pennsylvania Police Department and its employees.

It shall also be the policy of the University of Pennsylvania Police Department that all existing laws, rules, regulations, and directives that govern on- and off-duty conduct are applicable to conduct associated with social media and networking.

III. Scope

This directive shall affect all sworn employees.

IV. Definitions

- A. **Electronic Resources:** For the purposes of this policy, electronic resources shall include the following University assets including, but not limited to, desk-top computers, lap-top computers, hand-held digital electronic devices, digital storage media, networks, electronic mail, electronic information and data, video and voice services, facsimile transmissions and mobile data terminals available to UPPD personnel.
- B. **Mobile Device:** Any portable device used to access University resources via a wireless connection (e.g. cellular, Wi-Fi, Bluetooth, AirPennNet, etc.).

- C. Jailbreak (Jailbroken): The process of attaining privileged control (known as "root access") of a device running the Apple iOS operating system that allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions.
- D. Root (Rooting, Rooted): The process of attaining privileged control of a device running the Android operating system that allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions.
- E. Electronic Mail: commonly referred to as email or e-mail, is a method of exchanging digital messages from an author to one or more recipients using a computer to computer (or cell phone) communication system. Email systems are based on a store and forward model; email servers accept, forward, deliver, and store messages.
- F. Internet: A global system of interconnected computer networks that use the standard internet protocol suite to facilitate data transmission and exchange.
- G. Criminal Justice Information Systems: Secure internet-base/accessed communications portals which allow criminal justice agencies to instantly access driver license and motor vehicle information, criminal history records, active warrants, stolen property records, protection from abuse orders and the missing persons database. These systems provide law enforcement with messaging capabilities and information sharing conduits.
- H. Social Media: On-line sources that allow people to communicate, share, and/or exchange information with others via some form of on-line or cellular network platform. Information may include, but is not limited to, text, photographs, video, audio and other multimedia files.
- I. Social Networking: Involves using such Internet or mobile formats as Facebook, Twitter, Instagram, LinkedIn, Foursquare, Usenet groups, message or on-line bulletin boards, blog and other similarly developed formats, to communicate with others using the same groups while also networking with other users based upon similar interests, geographical location, skills, occupation, ideology, beliefs, etc.
- J. Post (Noun): An item inserted into a blog, or an entry to any type of computerized bulletin board, forum or social media site.
- K. Post (Verb): The act of creating, uploading, editing or adding to any social media outlet. This includes text, photographs, audio, video or any other multimedia file.
- L. Blog: A series of entries, written by either one person or a group of people, in an online journal, usually posted in chronological order, like a diary. Blogs can allow or disallow comments on entries.
- M. Comments: Responses to a blog post, news article, social media entry or other social networking post.

V. Procedures

A. Implied Consent

1. Each person with access to the University's computing resources is responsible for their appropriate use and by their use agrees to comply with all applicable University, School, and departmental policies and regulations, and with applicable City, State and Federal laws and regulations, as well as with the acceptable use policies of affiliated networks and systems.

B. General Use of Electronic Resources and Assets

1. This policy shall apply to the use of electronic resources by UPPD personnel including but not limited to the following circumstances:
 - a. Resources accessed on or from University premises;
 - b. Resources accessed using University owned computer equipment or University access methods or conduits;
 - c. Resources used in a manner that identifies the employee with the department;
 - d. Resources used for communications that make reference to the department.
2. The University of Pennsylvania strives to provide a reasonable level of privacy; however, users should be aware that any data created using University owned electronic resources remains the property of the University of Pennsylvania.
3. The use of University computer resources for private business or commercial activities (except where such activities are otherwise permitted or authorized under applicable University policies), fundraising or advertising on behalf of non-University organizations, or the reselling of University computer resources to non-University individuals or organizations, and the unauthorized use of the University's name, are prohibited, unless specifically authorized by the Vice President for Public Safety and the Chief of Police.
4. Users shall not set any rules within their email software to forward UPPD email to non-University email servers or accounts.
5. The General Standards for the Acceptable Use of Computer Resources require:
 - a. Responsible behavior with respect to the electronic information environment at all times;
 - b. Behavior consistent with the mission of the University of Pennsylvania Police Department and with authorized activities of the University or members of the University community;

- c. Respect for the principles of open expression;
 - d. Compliance with all applicable laws, regulations, and University policies;
 - e. Truthfulness and honesty in personal and computer identification;
 - f. Respect for the rights and property of others, including intellectual property rights;
 - g. Behavior consistent with the privacy and integrity of electronic networks, electronic data and information, and electronic infrastructure and systems; and
 - h. Respect for the value and intended use of human and electronic resources.
6. Employees shall exercise good judgment in use of all University owned or related resources whether on or off duty.
 7. The use of electronic resources while on duty, including e-mail and internet use should be kept to a minimum and should never interfere with work responsibilities.
 8. Personnel are responsible for the security of any University owned electronic resource or asset under their control or in their possession.
 - a. No University, UPPD or DPS asset shall be left unattended or stored inside of personal vehicles.
 9. No University owned electronic asset may be moved or taken off the premises of the Division of Public Safety Building without prior permission from the Chief of Police or designee.
 - a. Any equipment loaned by DPS remains the property of DPS, and therefore the borrower is responsible for the care and return of this equipment. Employees, upon demand, must produce the loaned equipment within 24 hours of the request for its return.
 10. A user's access to University owned electronic resources may be immediately suspended for violations of this policy.
 11. Department of Public Safety personnel are authorized to immediately remove any electronic resource from the University network if deemed a risk to the environment.
- C. Software and Security
1. Only authorized software programs or other files may be introduced to University owned desk-top or portable computers, including mobile data terminals.
 - a. Portable data disks or storage media shall not be utilized on any University owned computers, including mobile data terminals without the prior consent of the Information Technology Support Specialist. These items will be inspected for virus

infection by the Information Technology Support Specialist prior to introduction into the department's computer system or stand-alone computers or laptops.

2. Authorized software may not be manipulated or altered on any University owned desk-top or portable computers, including mobile data terminals.
3. Only licensed software, being utilized for its intended application, shall be permitted for use on University owned resources. The Information Technology Support Specialist for the University or DPS shall ensure that all software programs are properly licensed and are only used for their intended application.
4. Users of University owned electronic resources shall immediately report any suspected virus activity or possible security compromise.
 - a. Request for software installation, repairs, routine maintenance, and modifications to University owned electronic resources shall be requested via the chain of command.
5. Each authorized user of University electronic resources shall be issued a login name and a temporary password.
 - a. Passwords must be at least eight (8) characters long; must not be simple, dictionary words; may not contain your login or full name; must contain a mix of alphabetic, numeric, and special characters (e.g. "*&^%\$%\$#"); and must change at least every ninety (90) days.
 - b. Users of University owned electronic resources are responsible for the security of their passwords and accounts, and should never share them with anyone, include other employees.
6. All information systems should be appropriately secured by logging-off or locking the console when left unattended.

D. Criminal Justice Information Systems

1. Authorized and trained UPPD personnel may be provided with access to Criminal Justice Information Systems for use ONLY while on-duty. Criminal Justice Information Systems include, but are not limited to the following:
 - a. National Crime Information Center (NCIC): The FBI provides a host computer and telecommunication lines to a single point of contact in each of the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, and Canada, as well as federal criminal justice agencies. Those jurisdictions, in turn, operate their own computer systems, providing access to nearly all local criminal justice agencies and authorized non-criminal justice agencies nationwide. The entry, modification, and removal of records are the responsibility of the agency that entered them. NCIC is an electronic

catalogue of crime available to virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year.

- b. Commonwealth Law Enforcement Assistance Network (CLEAN): The Pennsylvania State Police provides the Commonwealth Law Enforcement Assistance Network (CLEAN) which is used by the Commonwealth's criminal justice agencies to access driver license and motor vehicle information, state criminal history record information maintained in the Pennsylvania State Police Central Repository, the Commonwealth's central registry for Protection from Abuse orders, "hot" (stolen and wanted) files, law enforcement messaging capabilities, and a host of other services. CLEAN is Pennsylvania's conduit to NCIC, the FBI's National Crime Information Center, and to the National Law Enforcement Telecommunications System (NLETS), which is the International Justice and Public Safety Information Sharing Network.
- c. Pennsylvania Justice Network (JNET): The Pennsylvania Justice Network (JNET) is the Commonwealth's primary public safety and criminal justice information broker. The JNET integrated justice portal provides a common online environment for authorized users to access public safety and criminal justice information. This critical information comes from various contributing municipal, county, state, and federal agencies.
- d. Philadelphia Crime Information Center (PCIC): The Philadelphia Police Department provides access to a host computer which is the central registry for crime data entered by Philadelphia Police Department personnel. Access to this system is limited to the Philadelphia Police Department and a regulated number of criminal justice agencies in Pennsylvania. Information in PCIC is entered into CLEAN and NCIC on a regular basis making the information readily available all authorized criminal justice agencies.
- e. Police Integrated Information Network (PIIN): The City of Philadelphia provides a network which allows for the electronic consolidation of arrest and/or discovery documents that can be retrieved by the Philadelphia District Attorney's Office for use in charging decisions and court proceedings. Authorized law enforcement personnel have access to the network and can create an electronic discovery package immediately following an arrest. The discovery package includes arrest reports, interviews and photos which are associated to a Philadelphia Police District (Incident) Control Number.
- f. Preliminary Arraignment Reporting System (PARS): The City of Philadelphia provides an electronic application which allows for the entry crime incidents and arrest information. The information is entered by authorized personnel and stored in a centralized database. The PARS application interfaces with Police Integrated Information Network (PIIN) and is used by law enforcement personnel to generate arrest reports; the PARS application is also utilized by the Philadelphia District Attorney's Office, the Philadelphia Public Defenders Office and the Philadelphia Court System from arrest through arraignment.

2. Access to NCIC, CLEAN, JNET and PCIC by patrol personnel shall be made ONLY through use of the mobile data terminals (MDT) installed in UPPD patrol vehicles or designated terminals located within UPPD HQ. Patrol personnel are not permitted to access these systems using any other computer or electronic device, unless authorized by the Chief of Police or designee. Access from a non-University owned terminal is strictly prohibited.
 - a. Access to Criminal Justice Information Systems by Detective and Supervisory personnel utilizing desk-top or lap-top computers is authorized.
3. Access to PARS and PIIN can only be made through via specific terminals located within UPPD Headquarters or PPD facilities.
4. Whenever NCIC, CLEAN, JNET and PCIC are utilized by UPPD patrol personnel an incident report (UPPD-10) must be completed. A copy of the printout from the system access shall be attached and submitted to Records with the associated incident report.
 - a. Access to NCIC, CLEAN, JNET and PCIC by patrol personnel is allowed ONLY when physically investigating a person or object.
 - 1) Only UPPD Detectives or other personnel as authorized by the Chief of Police are permitted access the systems for investigative purposes.
 - b. Whenever patrol personnel access any of the above listed systems utilizing mobile data terminals (MDT), an incident report (UPPD-10) must be completed. The incident report (UPPD-10) must include the reason for the access and the results of the specific inquiry. The Police Operations Room Supervisor will ensure that all usages of the MDT are noted on the specific incident report. The Police Operations Room Supervisor shall also have the PennComm Operations Room Supervisor check the information listed on the incident report through the PennComm access to Criminal Justice Information Systems. A copy of the printout from the access by PennComm must be attached to the incident report and submitted to Records.

E. Prohibited Activities

1. The following activities are prohibited when using any University owned electronic resources including, but not limited to, computers, computer software, e-mail, internet access and other electronic equipment:
 - a. Conducting illegal activities or making available any materials the possession or distribution of which is illegal;
 - b. Engaging in any activity for personal gain or profit;
 - c. Engaging in political activities or any other activities which violate any UPPD or University Policy;

- d. Accessing, sharing, downloading, storing, or printing pornographic material;
- e. Gambling, wagering, betting, or selling chances;
- f. Revealing or publicizing copyrighted, proprietary, or confidential information that is not authorized;
- g. Intentionally compromising or allowing unauthorized access, possession, or distribution, by electronic or any other means, of electronic information or data that is confidential under the University's policies regarding privacy or the confidentiality of student, administrative, personnel, archival, or other records, or as determined by the Vice President for Public Safety and Chief of Police;
- h. Intentionally damaging or destroying the integrity of electronic information;
- i. Making improper remarks or proposals (improper remarks include those that contain defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, discriminatory, or illegal material);
- j. Representing personal opinions as those of the University of Pennsylvania, the University of Pennsylvania Police Department or The Division of Public Safety;
- k. Using, acquiring, or attempting to acquire passwords/accounts of others;
- l. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for University resources or Criminal Justice Information Systems;
- m. Misrepresentation (including forgery) of the identity of the sender or source of an electronic communication to include anonymous or pseudonymous communications.
- n. Alteration of the content of a message originating from another person or computer with intent to deceive;
- o. Intentionally infringing upon the intellectual property rights of others, including plagiarism and unauthorized use or reproduction.
- p. The interception or attempted interception of communications by parties not explicitly intended to receive them without approval of an authorized University official;
- q. The use of restricted-access University computer resources or electronic information without or beyond one's level of authorization;
- r. Accessing Criminal Justice Information Systems while off-duty, on restricted duty or in violation of any provisions of this policy;

- s. Making University computing resources available to individuals not affiliated with the University of Pennsylvania without approval of an authorized University official;
 - t. The unauthorized copying or use of licensed computer software;
 - u. Intentionally or negligently disrupting or causing interference with the use of electronic networks, information systems/resources and/or users; including, but not limited to, the propagation of computer "worms" and "viruses", the sending of electronic chain mail, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts;
 - v. Altering or attempting to alter files or systems without authorization;
 - w. Unauthorized scanning of networks for security vulnerabilities;
 - x. Attempting to alter any University computing or networking components (including, but not limited to, bridges, routers, and hubs) without authorization or beyond one's level of authorization;
 - y. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer or network services; and
 - z. Negligence leading to the damage of University electronic information, computing/networking equipment and resources.
2. The use of "Jailbroken", "Rooted" or similarly modified mobile devices to access University owned electronic resources or networks is strictly prohibited.
 3. Failure to comply with requests from appropriate University/DPS officials to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this policy.

F. Electronic Mail (E-Mail) Communications

1. Each employee shall be assigned a University of Pennsylvania Department of Public Safety email account. E-mail is ONLY to be used for official UPPD business and is the property of the University of Pennsylvania; it is not a private account and is therefore subject to monitoring by University officials.
2. UPPD/DPS e-mail addresses identify the organization that sent the message; therefore, users should consider e-mail messages to be the equivalent of letters sent on official letterhead. Users should not regard e-mail, particularly internet e-mail, as a secure form of communication. Even e-mail secured with encryption technology can be shared with others in print or by being forwarded. Users should carefully consider whether e-mail is the appropriate medium when they desire confidentiality.

3. The use of University e-mail accounts for personal gain, personal business, commercial advantage, solicitation for any person or non-profit, advocacy of a cause or special interest, political advantage, or any unlawful purpose is prohibited.
4. All UPPD employees **are required** to check their e-mail On Each Workday for training bulletins, notifications or information items addressed to them personally, or via group e-mail.
 - a. Personnel shall be allotted reasonable time to complete this task during their tour of duty.
 - b. Computer access terminals shall be designated for this purpose inside of the Division of Public Safety Building, 4040 Chestnut Street.
 - c. Personnel are required to open interdepartmental emails whether or not they are tracked.
5. All sworn personnel shall follow correct escalation procedures for corresponding with UPPD supervisory personnel, DPS Directors / employees, including University Officials. All e-mails must be submitted using the appropriate chain of command.
6. All communications written or forwarded via e-mail shall be professional, appropriate and lawful. The forwarding of chain letters or “spam” is strictly prohibited.
 - a. All electronic communications shall be treated with the same degree of propriety and confidentiality as official written correspondence or verbal communication.
 - b. Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications (as defined by law), are prohibited.
 - c. The use of University computer resources for private business or commercial activities (except where such activities are otherwise permitted or authorized under applicable University policies), fundraising or advertising on behalf of non-University organizations, and the unauthorized use of the University's name, are prohibited unless expressed permission is given by the Vice President for Public Safety and Chief of Police.
7. E-mail signatures must be uniform and accordance with DPS Policy #009, Division Email Signature Policy. (See appendix “a”).
8. Personnel shall not allow unauthorized persons to use any University owned electronic resources including email, without expressed permission from the Chief of Police or designee.
9. Confidential, proprietary or sensitive information may only be disseminated 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. Personnel information
- b. Complaints
- c. Grievances
- d. Misconduct
- e. Discipline
- f. Medical records
- g. Crime scenes
- h. Criminal history
- i. Operations Orders
- j. Intelligence files

10. Personnel are responsible for the security of the email system by not leaving computers unattended when e-mail is active and by not sharing passwords.
11. Personnel shall not send emails or other electronic messages under another user's name, including the sending of anonymous or pseudonymous messages.
12. DPS IT support and troubleshooting is only available during normal business hours. Personnel in need of support after normal business hours shall submit a memo to the Captain of Staff and Administrative Services via the chain of command.
 - a. Contact with DPS IT personnel shall only be conducted through an on-duty supervisor.
 - b. DPS IT personnel shall not be contacted after hours.

G. Internet Usage

1. The use of University provided electronic resources is for the purposes of conducting official University of Pennsylvania business. However, authorized personal use of the internet is permissible on a limited basis as determined by the Chief of Police or designee. Authorized personal use of the internet shall be used in such a way that it does not interfere with an officer's responsibilities as a member of the UPPD.
 - a. Internet access should be limited to work related sites, with the exception of accessing weather information, news and directions.

2. The internet is not a secure means of transmission; Internet communications through University electronic resources are subject to audit and discovery in law proceedings.
3. The University has the right and capability to monitor internet browsing by each user on our system. The Internet is a privilege. Downloading programs from the Internet is strictly prohibited without the express consent of the Chief of Police or designee.
4. Employees have no proprietary interest and no reasonable expectation of privacy while utilizing any of the University owned resources including but not limited to, computers, computer software, networks, e-mail or other electronic equipment provided by the University. The University owns and is responsible for the computers, computer software, internet connection and other electronic equipment provided by the University and may inspect, repair, perform maintenance on, or search any computer owned by the University at any time, for any reason, including criminal investigations.

H. Mobile Devices

1. Personnel may use mobile devices to access University resources via AirPennNet or other secured networks in order to log onto University e-mail or websites.
 - a. The use of mobile devices to access Criminal Justice Information Systems or any confidential or sensitive information is strictly prohibited.
2. It is strictly prohibited for mobile devices to contain University information that may be considered sensitive such as social security numbers, health information, salary, disciplinary action, account passwords or any information that if compromised could cause significant harm to an individual or the University.
 - a. Personnel must immediately notify their immediate supervisor if a mobile device with the potential to expose sensitive information is lost.
3. The University reserves the right to wipe lost or stolen devices if necessary to protect confidential University data contained on the device, whether or not the device is owned by the University.
 - a. A device wipe could occur upon separation of service from the University. Depending upon the technical implementation, this could result in all data stored on a device being wiped;

I. Mobile Data Terminals

1. The University of Pennsylvania Police Department provides authorized personnel with access to Criminal Justice Information Systems, the Division of Public Safety PennComm Computer Aided Dispatch (CAD) system and limited internet connectivity through a patrol vehicle mounted mobile data terminal (MDT).

2. Personnel authorized to utilize mobile data terminals shall do so in compliance with this policy.
3. Mobile data terminals shall be primarily used by patrol personnel to access Criminal Justice Information Systems in order to investigate persons and vehicles while conducting traffic enforcement or other duties related to their patrol assignment.
4. The use of the MDT to conduct "Moving Motor Vehicle Checks" is a valuable and discretionary police tool, but shall not be used as a replacement for reasonable suspicion or probable cause to initiate a motor vehicle investigation or investigation of a vehicle's occupants.
 - a. This method of information gathering will ONLY be used at the discretion and approval of the Shift Commander/Supervisor after he/she has acquired the pertinent facts about an officer's request to receive a BMV check.
 - b. Officers must submit a UPPD Incident Report (UPPD-10) for all "Moving Motor Vehicle Checks" regardless of whether or not the vehicle in question was actually stopped by the officer.
5. The MDT shall not be used by the operator of a patrol vehicle while the vehicle is in motion.
6. Whenever patrol personnel access any of the Criminal Justice Information Systems via mobile data terminals (MDT), an incident report (UPPD-10) must be completed in accordance with section V.D.4.b. of this policy and notify the PennComm dispatcher of the location of the investigation.
7. Untrained users are not permitted to access or utilize the MDT in any fashion.
8. Personnel shall ensure the security of the MDT by logging-off or locking the console when left unattended.
 - a. Vehicles with an MDT installed shall be secured at all times when unattended. Mobile data terminals shall be removed from vehicles that are placed out of service or that are down mechanical.
9. Malfunctions, damage, theft or security breaches related to the MDT shall be immediately reported to an on-duty supervisor.

J. Training

1. All employees authorized to use University owned resources shall be trained on the use of the equipment, access to the software, network and applications they are authorized to use.

2. The UPPD training division shall ensure that all personnel authorized to access University owned resources are provided with updated training and/or recertification as it becomes available.
3. Remedial training may be provided for personnel upon request or at the direction of the Chief of Police or designee.

K. Use of Social Media and Networking (General)

1. All personnel are prohibited from using University of Pennsylvania resources (on or off duty) to engage in personal use of social media.
2. All on duty personnel are prohibited from using privately-owned property/resources to engage in the personal use of social media.
3. All personnel are prohibited from posting, placing or having posted or placed by a third party any information relating to their duties or any information they have learned as a result of their duties as an employee of the University of Pennsylvania Police Department on any social networking site. This prohibition shall include, but not be limited to:
 - a. The posting of any pictures, video, audio, comments, discussion, or other digital technology media of any incident, inquiry, investigation, or all other information relating to the University of Pennsylvania Police Department.
4. All pictures, audio or video recorded, collected, captured, or stored by an officer during an officer's tour of duty, which is related to any official business of the University of Pennsylvania and/or specifically the officer's duty, is the property of the University of Pennsylvania Police Department whether the employee utilizes departmental equipment or equipment owned by the officer or another person. The officer shall ensure that digital technology collected as evidence or digital technology that has or may have evidentiary value is treated, collected, stored, and documented as evidence, in accordance with UPPD Written Directive 38 "Property and Evidence Control".
5. All pictures, audio, or video recorded, collected, captured, or stored by an officer during an officer's tour of duty, which is related to any official business of the University of Pennsylvania and/or specifically the officer's duty shall not be forwarded or provided in any manner to any person without the approval of the Chief of Police or designee.
 - a. All UPPD employees must be aware that use of personally owned equipment to collect digital technology may be considered evidence and the equipment or its contents may be inspected, seized or held as evidence.
6. Employees of the University of Pennsylvania Police Department, while on or off duty, shall never utilize digital technology, blogs, or social networking sites to harass, belittle or criticize an employee or another person in any manner. The posting of any digital technology to a social networking site or forwarding or sending an email(s) or text(s) that

criticizes, ridicules, or otherwise may potentially embarrass or disgrace another employee or person is prohibited. This shall also include the altering or editing of digital technology that harasses, belittles, or criticizes an employee in any manner.

L. Department-Authorized Use of Social Media and Networking

1. Department-authorized use of social media is defined as the employment of such instruments for the specific purpose of assisting the department and its personnel in community outreach, problem-solving, investigation, crime prevention and other department-related objectives.
2. In addition to the rules and regulations set forth in this directive, the following provisions shall apply to department-authorized use of social media.
 - a. Police department employees seeking to represent the department via social media outlets (e.g., individual or unit web page, Facebook, Twitter, etc.) shall obtain express permission from the Chief of Police or his/ her designee, prior to engaging in such activity.
 - b. Upon obtaining authorization, when engaging in social media networking, employees shall:
 - 1) Properly identify themselves as a member of the department.

Note: In instances whereby proper identification poses a risk to officer safety or may impede the progress of a criminal investigation, employees, with permission from the Chief of Police or his/her designee may exclude department membership from their profiles.

- 2) At all times, conduct themselves as representatives of the department and, accordingly, adhere to all department policies and standards of conduct, and observe conventionally accepted protocols and proper decorum.
 - 3) Observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.
 - 4) Observe and abide by all provisions of this directive regulating the use of University resources.
 - 5) Strictly adhere to existing federal, state, and local laws including laws regarding public information on arrests, investigations and personal data; policies of the University of Pennsylvania and University of Pennsylvania Police Department.
- c. When engaging in department-authorized social media networking, department employees shall not under any circumstances:

- 1) Make statements about the guilt or innocence of any suspect or arrestee or comments concerning pending prosecutions.
- 2) Post, transmit, or otherwise disseminate confidential information, including photographs or videos related to department training, activities, investigations, or any other work-related assignment, without specific and express written permission from the Chief of Police or his/her designee.
- 3) Conduct political activities or private business.

M. Personal Use of Social Media and Networking / Off Duty Conduct

1. Personal use of social media is defined as engagement or participation in any personal social networking platform, including but not limited to, personally owned sites, the sites of others (both known and unknown to the employee), news media pages and professional sites unaffiliated with the University of Pennsylvania Police Department or other information exchange forums.
2. Employees of the University of Pennsylvania Police Department are held to the highest ethical standard, which is an inherent part of the law enforcement profession. An officer's conduct, both on and off duty, is the means by which the officer and the police department's reputation are measured.
3. Employees who are off duty and using privately owned property to engage in the personal use of social media, do not represent the University, University of Pennsylvania Police Department or any official position maintained by either entity. Under such conditions, employees represent only themselves and their personal interests.
4. Officers must maintain high standards of professional and personal conduct at all times. Employees utilizing, posting pictures/audio/video, commenting, or creating a social networking site(s), blogs, and comment oriented websites, must conduct themselves at all times in a manner so as to not bring embarrassment, disgrace, or doubt as to their credibility as an impartial police officer or employee of the UPPD, or does not bring discredit upon individuals, the Department, the University of Pennsylvania or the community.
5. Employees will often find that their status as a police employee or their duty to act as a police officer while off duty enables them to view, assist, or become involved in critical incidents. When this occurs, officers shall conduct themselves in accordance with this policy in terms of their use of digital technology in the same manner as if they were on duty.
6. In addition to the rules and regulations set forth in Section V., Subsections I. and J. of this directive, the following provisions shall apply to personal use of social media while off-duty and using privately-owned property.
 - a. Employees shall neither express nor imply that they are:

- 1) Speaking or acting on behalf of the police department.
 - 2) Representing or presenting the interests of the police department.
- b. Employees shall not use their rank, title, or position in a manner that would suggest that they are representing the interests or official position of the police department.
- c. Employees shall not post any text, photograph, video, depiction or illustration of the Official Seal of the University, Division of Public Safety or the University of Pennsylvania Police Department name, badge, logo, patch, or patrol vehicle, so as to give the appearance of an official site of the University, Division of Public Safety or the University of Pennsylvania Police Department.
- d. In addition to the above provisions, when engaging in personal use of social media, employees shall not post any text, photograph, audio, video, illustration, or any other multimedia file related to, or depicting, any of the following:
- 1) Current, past, or pending departmental investigation.
 - 2) Criminal or civil proceeding pertaining to or arising from any matter involving the department, including allegations of misconduct.
 - 3) Brandishing of any weaponry (UPPD-owned or privately-owned; actual or simulated), or any contraband (actual or simulated).
 - 4) Brandishing of tactical instruments (both UPPD-owned and privately-owned), including but not limited to firearm, ASP, baton, OC spray, Electronic Control Weapon (ECW), and mechanical restraints.

N. Investigations

1. The UPPD may access, for quality control purposes and/or for violations of this policy, electronic transmissions, of members utilizing University owned electronic resources.
2. Employees who are subject to internal investigations may be ordered to provide the department with access to a social networking site(s) when the subject of the investigation is directly, narrowly, and specifically related to the employee's performance or ability to perform his or her function within the department or when the subject of the investigation is potentially adverse to the operation, morale, or efficiency of the department.
3. Candidates seeking employment with the University of Pennsylvania Police Department may be required to provide the department with access to any social networking site(s) in which they participate as a part of any background investigation.

O. Privacy

1. Users of University owned electronic resources shall immediately report any suspected virus activity or possible security compromise.
2. Users of University owned electronic resources are responsible for the security of their passwords and accounts.
3. All of University owned electronic resources should be appropriately secured by logging-off or locking the console when left unattended.
4. Employees should be aware that they may be jeopardizing their personal confidentiality and/or that of other employees by posting photographs or personal information about themselves or other members of the University of Pennsylvania Police Department.
 - a. This activity may jeopardize their safety, the safety of their family, their co-workers, and on-going or future investigations. Furthermore, employees are advised that in the event information has been posted on a social networking site identifying themselves as a police officer, the posting could make them ineligible for specialized assignments where anonymity is required.

P. Compliance

Violations of this directive, or portions thereof, may result in disciplinary action.

Q. Officers Assigned to Other Agencies

Officers of this department assigned to or assisting other law enforcement agencies will be guided by this directive.

R. Application

This directive constitutes departmental policy, and is not intended to enlarge the employer's or employee's civil or criminal liability in any way. It shall not be construed as the creation of a higher legal standard of safety or care in an evidentiary sense with respect to third party claims insofar as the employer's or employee's legal duty as imposed by law. Violations of policy will only form the basis for departmental administrative sanctions. Violations of law will form the basis for civil and criminal sanctions in a recognized judicial setting.