The Allegheny County Chiefs of Police Association

MODEL
INFORMATION TECHNOLOGY
INTERNET & SOCIAL MEDIA POLICY

An Allegheny County Criminal Justice Advisory Board Project

Initial issue 2016 reissued 2021, 2024

In Partnership With
The Allegheny County District Attorney's Office
October 2024

This model should serve only as a "**Starting Point**" for those departments who may wish to update their Rules & Regulations Manual in this area. To best serve your department, it should be reviewed and revised by you and your Municipality and Insurance Carrier.

01. PURPOSE

a. The purpose of this policy is to provide all Members of the Department with guidelines on the responsible and productive use of Department Information Technology and possible related activity including internet and social media (on-duty & off-duty) use. Changes in technology, law and procedure may give rise to future modifications and updates.

02. POLICY

a. Department policy prohibits discrimination against any person because of age, race, color, creed, religion, sex, sexual orientation, national origin, ancestry, marital status, physical or mental disability or medical condition.

b. A member's off-duty conduct shall be governed by this policy to the extent that it is related to act(s) that may materially affect or arise from the member's ability to perform official duties or to the extent that it may be indicative of unfitness for his/her position.

c. Failure of any member to meet the guidelines set forth in this policy, whether on-duty or off-duty, including words, actions, and social medial posts may be cause for disciplinary action.

d. Any departure from this policy is only permitted with approval from the Chief or D/Chief.

03. ELECTRONIC MAIL

a. The electronic mail system @sample police.pa.us is the property of the Department and intended for official use only.

b. All messages composed, sent or received on the electronic mail system are and remain the property of the Department. They are not the private property of any employee. All users of the electronic mail system, by virtue of their use of the system, waive any right of or expectation to privacy to all electronic mail communications and attachments sent or received. The Department reserves the right to review, audit, intercept and access all messages created, received or sent over the electronic mail system for any purpose.

c. Any communication by electronic mail should be drafted with the same care as a formal memorandum and should not contain insensitive or off-color remarks that might potentially be embarrassing to the sender, the receiver, the Department or the public.

d. The electronic mail system shall not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, weight, sexual orientation, religious or political beliefs, national origin or disability.

e. Pornography or any material (visual or sound) that could reasonably deemed to be offensive under the Department Policy Prohibiting Unlawful Harassment shall not be stored or accessed via any portion of the Department Information Technology Systems. Access to web sites, newsgroups, chat rooms, and e-mail containing these materials is also prohibited.
***Exception*:** Members involved in criminal investigations involving computer crimes that require access to such sites must notify the Chief or D/Chief.

f. If an email containing material prohibited under this policy is received, delete it. If the sender is known, advise that sender to not send similar material again. If the Sender is unknown, click on the Junk button and select BLOCK SENDER. If you should continue to receive inappropriate emails from the Sender, notify the Chief or D/Chief.

g. The electronic mail system shall not be used to solicit for commercial ventures, religious or political causes or outside organizations.

h. As noted above, the electronic mail system shall be used for official business purposes only. Occasional personal use of the department's computers may be permitted, but the department may, at any time, monitor or restrict such personal use. Again, employees shall not have any expectation of privacy with respect to personal information stored or accessed on Department computers or computer storage medium, such as hard drives, flash drives, discs, compact discs, etc. Employees taking advantage of this occasional personal use of the Department's computers shall limit their time spent doing so, and shall not be derelict in their normal job responsibilities.

i. The electronic mail system does not guarantee privacy or confidentiality. Electronic mail may be at risk of detection by third parties or subjected to Right To Know (RTK) requests. Employees should use discretion when transmitting confidential information via electronic mail.

j. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.

k. All material generated by computer, voice mail, e-mail, and all inter Department communication should be treated as confidential by other employees and accessed only by the intended recipient.

l. Unauthorized access or entry into any other employee's computer, email and files is strictly prohibited.

04. INTERNET USAGE

a. Internet access to global electronic information resources on the Internet is provided by the Department to assist employees in obtaining work-related data and technology. Users must remember that all activities from a Department internet account will be perceived as activities authorized by the Department.

b. Internet access through Department equipment during working hours should be limited to official business purposes. Occasional access to the internet for personal use may be permitted but the Department may, at any time, monitor or restrict such personal use. Employees who choose to take advantage of this occasional personal use of the internet also waive any right of or expectation to privacy. Employees taking advantage of this occasional personal use of the internet shall limit their time spent doing so, and shall not be derelict in their normal job responsibilities.

c. Internet access through official equipment, after working hours, is permitted but shall adhere to the Internet content guidelines of this policy.

d. Internet use is prohibited for sites containing adult content, hate speech, criminal activity, violence, illegal drugs and hacking. Access to these sites for investigative purposes can be granted with approval from the Chief or D/Chief. Use on Internet access through Department equipment for any illegal purpose is prohibited. These prohibited categories may be modified at any time with notice from the Chief or D/Chief.

e. Users shall not view, download, copy, send, post, or access information that is illegal or obscene.

f. Employees must ensure that the use of the internet does not compromise the security and integrity of the Department network. Downloading unapproved files (ex. MP3's) and software is strictly prohibited without approval from the Chief or D/Chief.

g. Employees shall not post any messages which contain abusive or objectionable language, defame, libel or infringe on the privacy rights of others.

h. The Internet does not guarantee privacy or confidentiality. Information transmitted over the internet may be at risk of detection by third parties. Employees should use discretion when transmitting confidential information on the internet.

i. The Department reserves the right to monitor internet usage, and inspect employee's computer systems for violation of this policy.

j. An alternate internet connection on any Department system is expressly prohibited without prior approval from the Chief or D/Chief.

k. This Department reserves the right to block an employee's internet usage due to violations of this policy.

05. SOCIAL MEDIA

a. Social media activity and speech as private citizens relating to matters of a public concern are First Amendment protected forms of speech. However, by virtue of the position, members of the Department are held to a higher standard than general members of the public, and any online activities should reflect such professional expectations and standards. Members are free to express themselves as private citizens on social media sites to the degree that their speech and/or language does not impair working relationships of the Department, impede the

performance of duties, impair discipline and harmony among coworkers, or negatively affect the public's trust and/or confidence in the Department. Members may be subject to disciplinary action for conduct unbecoming an officer, intemperance, or immorality for off-duty actions.

b. Members should be cognizant of the fact that their social media activity, even on personal social media accounts, may be seen by the public as a statement on behalf of the Department. Any activity that can be linked to a member is a reflection of the Department as a whole.

c. Members are accountable for their conduct, including the use of personal social media accounts. Members should be aware that statements made on social media sites are done so in an online domain where no reasonable expectation of privacy exists. Members creating or belonging to "private" or "limited access" accounts, with customized privacy settings must know that any statements, posts, videos, photographs, etc., that are shared via that account on the internet, may still be disseminated by third parties, even after the content has been edited or deleted by the user.

d. Members must be aware that information, including digital images, released on social media, may endanger the safety of members and/or their family members.

e. Members are cautioned that as public employees speech made pursuant to their official duties, whether on or off duty, is not protected under the First Amendment and may be subject to discipline if it is deemed detrimental to the Department. The on and off-duty conduct of members may reflect on the Department's reputation.

f. Members are prohibited from using any social media or social networking platform accessed through Department Information Technology while on duty, unless permission is granted from the Chief or D/Chief for investigative or public information purposes. Members are prohibited from using any social media or social networking platform accessed through personal devices other than Department Information Technology while on duty, unless permission is granted from the Chief or D/Chief for investigative or public information purposes.

g. Unless granted explicit permission from the Chief or D/Chief, Members are prohibited from posting either while on duty or off duty, any of the following on any social networking platform, either on their own sites, the sites of others known to them, the sites of others unknown to them, news media pages, or other information exchange forums:

1. Any text, photograph, audio, video, or any other multimedia file related to any investigation, both current and past, of this Department.

2. Any text, photograph, audio, video, or any other multimedia file related to any past or current action of this Department, either in homage or critique.

3. Logos, badges, seals, uniforms, vehicles, equipment or any item or symbol that is affiliated with this Department.

4. Any item, symbol, number, or likeness or material that is identifiable to this Department.

5. Any text, photograph, audio, video, or any other multimedia file that is related to any investigation/prosecution by the Department.

h. Members who choose to maintain or participate in social media or social networking platforms while off duty shall conduct themselves with professionalism and in such a manner that will not reflect negatively upon the Department or its' mission. In the course of operating or participating in such forums, the following rules shall apply:

1. Unless explicitly granted permission by the Chief or D/Chief, Members shall not identify themselves, in any way, directly or indirectly as an employee of this Department.

2. Members shall not use any reference to infer they are employees of this Department.

3. Members will be held responsible for the content that appears on their maintained social media or social networking sites and will be obligated to remove any posting or material contributed by others that identifies the Member as an employee of the Department, or reflects negatively upon the Department or its mission.

4. Sexually graphic or explicit material of any kind shall not be posted or shared by Members on any form of social media or social networking site. Any posting or material of such contributed by others shall be immediately removed from your site.

5. Any content involving discourteous or disrespectful remarks pertaining to issues of ethnicity, race, religion, gender, gender identity/expression, sexual orientation, and/or disability shall not be posted or shared by Members on any form of social media or social networking site. Any posting or material of such contributed by others shall be immediately removed from your site.

6. Members shall not post, transmit, share, and/or disseminate any content advocating harassment or violence. Any posting or material of such contributed by others shall be immediately removed from your site.

7. Weaponry, owned by this Department and/or owned personally or privately by Members shall not be displayed or referred to, in any social media forum if such displays or depictions promote or glorify violence.

8. Members shall not post, transmit, share, and/or disseminate any content that is defamatory, pornographic, proprietary, harassing, or libelous. Any posting or material of such contributed by others shall be immediately removed from your site.

9. Members shall not engage in any type of social media contact (friending, following, etc.) with an actor, suspect, witness, crime victim, or attorney, involved in the same case, if that Officer was either involved in the incident, or the Officer became acquainted with person during or because of the incident, and the matter is ongoing.

10. Members shall not engage in any type of social media contact (friending, following, etc.) with minors they interact with in the course of their employment with the Department.

11. Any posting that detracts from the Department's mission will be considered a direct violation of this policy.

i. Unless serving as an explicitly permitted tool of public information or community outreach, no Member shall use their rank and/or title in any social media or social networking activity, including inclusion of said rank and/or title into the Member's online identity or avatar.

06 Definitions

Social Media: a variety of online internet sources that allow people to communicate, share information, share photos, share videos, share audio and exchange text and other multimedia files with others via some form of online or cellular network platform.

Social Networking: using or creating such Internet or mobile formats including but not limited to Facebook, Twitter, MySpace, Linkedln, Foursquare, Gowalla Police Pulse, The Squad Room, Usenet groups, Snapchat, online forums, message boards or bulletin boards, blogs and other similarly developed formats, to communicate with others using the same sites.

Mobile Social Networkings: social networking using a mobile phone or other cellular based device.

Blog: a series of entries on an internet site, 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 comments on entries or not.

Blogging: to read, write or edit a shared online journal. Blogging can also encompass the act of commenting- and engaging with other commenters - on any blog, including one operated by a third party.

Post: an item inserted to a blog or an entry to any type of computerized bulletin board or forum.

Forum: an online discussion site.

Comments: responses to a blog post, news article, social media entry or other social networking post.

Commenting: the act of creating and posting a response to a blog post, news article, social media entry or other social networking post. Commenting can also entail the act of posting an original composition to an unrelated post or article.

Avatar: a computer user's representation of himself/herself, or of an internet identity or alter ego.

Identity: an online identity, Internet identity or Internet persona that a social networking user establishes. This can be a real name, an alias, a pseudonym or a creative description.

Handle: the name of one's online identity that is used most frequently.

User Name: the name provided by the participant during the registration process associated with a Web site that will be displayed publicly on the site.