DEPARTMENT OF THE ARMY
US ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON
3312 A AVENUE, SUITE 208
FORT LEE, VA 23801-1720

IMLE-ZA

AUG 2 5 2020

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Fort Lee Social Media

1. REFERENCES.

a. Department of Defense Instruction 8550.01, DoD Internet Service and Internet-Based Capabilities, 11 September 2012.

b. Secretary of the Army Memorandum, Delegation of Authority, Approval of External Official Presences, 2 December 2013.

c. Office of the Chief of Public Affairs Memorandum, Standardizing official U.S. Army external official presences (social media), 10 January 2014.

d. CIO/G6 Memorandum, Responsible Use of Internet Based Capabilities, 25 March 2010

e. AR 360-1, The Army Public Affairs Program, 25 May 2011.

f. The United States Army Social Media Handbook: www.army.mil/socialmedia.

g. AR 530-1, Operations Security, 26 September 2014.

2. PURPOSE. To establish requirements and guiding principles for the implementation and effective use of official U.S. Army social media sites (also known as External Official Presences, or EOPs) by Fort Lee organizations, and set standards of conduct for participation by personnel on official sites.

3. APPLICABILITY. This policy applies to commanders and Fort Lee personnel who are authorized to create and manage official social media sites (e.g. Facebook, Twitter, YouTube, Instagram, etc.) for U.S. Army organizations on Fort Lee in accordance with Army guidelines. All personnel managing official social media sites must understand and follow these important guiding principles.

4. POLICY. Social media is a powerful communications tool. When used correctly, social media can help an Army organization reach an enormous audience. The guidelines set forth in this policy reinforce and build on those in the comprehensive Army Social Media Handbook and help to ensure the official use of social media presences by Fort Lee-based Army organizations is necessary and effective.

a. Establishing an EOP. As of 2019, approximately 80% of the U.S. population has established a social media account, and nearly half of the world's population is online. Social media presences are excellent communication tools when used effectively. Effective social media management requires command approval, training, the formation of strategy and goals, regular content creation and/or content management, interactive communication, and proper oversight. Ineffective and/or inactive social media presences frustrate interested audiences and may harm the credibility of an organization. Consider the following:

(1) Will my organization communicate better with internal and external stakeholders through the use of an EOP? Create a strategy and establish goals for the presence specific to the communication objectives of the organization.

(2) Will the EOP reach my organization's intended audience? Identify your organization's target audience. For example, audiences with an older demographic are more likely to be on Facebook than younger audiences.

(3) Does my organization have the time and resources to dedicate to a social media presence? EOPs should only be established with the full command and staff support required to operate effectively. Regular posts (at least one post weekly) and timely responses to questions and comments (within two hours during normal operating hours) on EOPs are vital to their effectiveness and value to the audience.

If "no" is the answer to any of the considerations above, organizations may benefit by providing their content to an existing social media presence (i.e. a higher headquarters EOP). If the answer is 'yes' to all considerations, the next step is to establish public affairs and command approval. Whenever the option is available, register the EOP with the Digital Media Division of the Office of the Chief of Public Affairs (brigade units and above) and as a government page with the social media platform.

b. EOP Administrators. EOP administrators are Soldiers or civilians who manage official social media presences for organizations or leaders, such as accounts on Facebook, YouTube, Twitter and Instagram. These accounts are considered official because they are created and managed using government resources to communicate the work of the Army. Social media managers play a powerful role in maintaining public trust and telling the Army story.

EOP administrators are expected to serve as subject matter experts on social media policies, techniques and best practices. Duties include actively engaging the public, promoting unity of voice, freedom of information, timeliness, and accuracy while maintaining security and privacy. EOP administrators are also required to complete annual training including:

(1) Operational Security for External Official Presence Operators: https://iatraining.us.army.mil

(2) DISA Social Networking Class: https://iatraining.disa.mil/eta/disa_sn_v21_fy17/launchPage.htm

The Department of Defense offers additional training resources to support EOP administrators including a social media training section from the Defense Information School (https://pavilion.dinfos.edu/Search-Results/Social-Media) and the DoD Social Media Hub (http://dodcio.defense.gov/Social-Media). A collection of best practices for government EOP administrators is available at www.digitalgov.gov.

CASCOM and Garrison PAOs may also provide social media administrator and awareness training to their supported organizations upon request.

c. Official Site Registration. The Garrison PAO is the lead for integrating communication among all installation partners. In order to maintain visibility of Fort Lee social media presences, facilitate a local social media community of practice and ensure continuity of operation for social media activity, all official U.S. Army social media presences managed by organizations on post are encouraged to register EOPs and provision administrator access to the Garrison PAO (this is required for Garrison organizations) in addition to registration requirements described in the Army Social Media Handbook. For Garrison organizations (optional for other Army organizations on post) this must be done after the establishment of a new EOP, and anytime there is an EOP administrator change or addition, by sending the following information via encrypted e-mail to ArmyFortLee.PAO@mail.mil:

(1) EOP URL and/or profile information.

(2) Rank, name, title, phone number and e-mail of EOP administrator(s).

(3) Proof of training completion by EOP administrator(s) (required annually).

(4) Following receipt of above, PAO will provide instructions for provisioning administrator access to the EOP and will then need confirmation it was granted.

Audits of Garrison social media presences may be conducted by PAO and/or the Office of the Chief of Public Affairs' Digital Media Division in accordance with Army policy, either annually or on an ad hoc basis. These audits ensure units are complying with applicable guidelines, SOPs, policies and regulations. Units are notified of violations found during the audits and asked to correct or respond to any issues. Posts on an account should be no older than one month, and the account should be updated on a weekly basis at minimum.

d. Content Approval. Release authority is a critical component of maintaining an EOP. Administrators should establish a method to ensure thorough content review before posting – being mindful of OPSEC, the Uniform Code of Military Justice, For Official Use Only documents, the Freedom of Information Act, etc. Content that should NOT be posted on official sites includes, but is not limited to: unit/personnel rosters; information, other than PAO-authorized releases, about personnel casualties; and details regarding active investigations. Most social media platforms allow for the sharing of content posted by others – be certain to only share accurate information from official sources. When in doubt about suitability of content for public release, administrators should contact their PAO for guidance.

e. OPSEC. Information that may compromise OPSEC should not be discussed via Army-managed social media. EOP administrators are solely responsible for monitoring sites, and documenting and removing any violations prior to reporting them to their organization's OPSEC officer or the Army's OPSEC program manager.

f. EOP Moderation. Ensure your social media presence includes rules of engagement (ROE) similar to those described in the Army Social Media Handbook. All online discussions and comments should be closely monitored by EOP administrators, but there should be a balance as not to over-moderate sites and conversations between users. Allow users connected to your EOP to fight your battles for you when possible. As they are not official representatives of the organization, they possess a different level of credibility that can help reinforce organizational values and positions. The following are considerations when properly moderating an EOP:

(1) Negative Comments. Do not shy away from negative comments. An open forum comes with certain risk of negativity and to avoid it can tarnish credibility. In addition, responses must be properly vetted / approved and accurately express the Army's position without editorializing or straying from the facts. Only delete or block comments or users when a clear pattern of malicious, derogatory behavior is apparent and they are in violation of the ROE. Do not delete comments simply because you do not like the message.

(2) Promotion and Endorsement. EOPs are not a place for personal or commercial advertisements nor endorsements. Administrators should remove any such content posted to EOPs.

(3) Protected Information. Social media content must respect copyright, trademark, privacy, fair use, financial disclosure and other applicable laws. Always give proper credit for another's work and make sure you have the right to use something, even with attribution. Do not publish pre-decisional or internal Army information unless authorized by the command. As a standard practice, avoid commenting on anything related to legal matters, ongoing investigations, litigation,

or any parties to litigation involving the Army. Always protect sensitive information, such as protected acquisition and personally identifiable information.

g. EOP Operation and Participation Principles. While a few of the following principles apply only to EOP administrators, some detail expectations for the online conduct of personnel on official sites or elsewhere online in an official capacity:

(1) Participate at your own risk, taking personal responsibility for your comments, your username, and any information provided.

(2) Stick to your area of expertise and provide unique, individual perspectives on what is going on at Fort Lee. Remember that only commanders and their PAOs are authorized to speak on behalf of the command.

(3) Post meaningful, respectful content - in other words, no spam, and no remarks that are off-topic or offensive.

(4) Pause and think before posting or responding to others. Reply to comments in a timely manner, when a response is appropriate. When disagreeing with others' opinions, keep it polite. What you write is ultimately your responsibility.

(5) Respect and protect proprietary information, content and confidentiality.

(6) Be transparent. Your honesty – or dishonesty – will be quickly noticed online. Do not lie or mislead people with your communications.

(7) Perception is reality. In online social networks, the lines between public and private, personal and professional are blurred. You create perceptions about yourself and Fort Lee simply by identifying yourself as a Soldier, employee or Family member affiliated with Fort Lee. What you post is viewable by commanders, supervisors and the public, so be sure all content associated with you is consistent with your values and professional standards, and those of the Army and Fort Lee. You might consider adding a disclaimer to all personal social media presences that states, "The views expressed are my own and in no way reflect the official position of any U.S. Government agency."

(8) Are you adding value? Social communication should be thought-provoking and build a sense of community. If your posts help people improve knowledge or skills, solve problems, or understand the Army and Fort Lee better, they are adding value. Talk online like you would talk to real people in person. Do not be afraid to bring in your own personality. Consider content that is open-ended and invites response.

(9) Be a Leader. There can be a fine line between healthy debate and incendiary reaction. Do not use social media to denigrate organizations or

individuals. Some topics slide very easily into sensitive territory, so be careful and considerate. Once your words are out there, you cannot get them back.

(10) All online conduct should be professional, especially for those in leadership positions. Written posts, photos and/or video, even when well-intentioned, can be misinterpreted. A good question to ask is, "Would it be OK if this appeared on the nightly news?" or "Would I say or do this in formation?" Do not allow something to be posted if it could be interpreted as inappropriate, or it may generate negative perceptions about you, Fort Lee or the Army.

(11) Using an official position to promote oneself online for personal or financial gain is inappropriate and can hurt the reputation of the Army and individual command.

(12) If it gives you pause, pause. If content you plan to post makes you even slightly nervous, take a minute to review these guidelines and figure out what is bothering you. Ultimately, what you publish is yours, as is the responsibility.

5. PROPONENT. The proponent for this policy is the Garrison Public Affairs Officer, (804) 734-7451/ ArmyFortLee.pao@mail.mil.

6. EFFECTIVE DATE. This policy becomes effective immediately upon signature.

KARIN L. WATSON
COL, MP
Commanding

DISTRIBUTION:
LEEKEY