Commanders are responsible for both their official external presence and for all social media platforms under their command. Echelon PAOs are authorized to release official information on their behalf and comply with the guidelines outlined in this regulation.

- Commanders at brigade level and above are encouraged to use social media platforms as part of their communication strategy. For lower echelon units, if the higher echelon PA office views the unit as having enough consistent content to warrant a separate social media presence, it will ensure the subordinate unit has the training and assistance needed to establish an effective social media program with the right platforms based on a communication plan. If the needs of a subordinate unit can be met with the higher echelon's social media presence(s), the subordinate unit should work with that PA office to coordinate content publication.

Functions

The OCPA Digital Media Division is responsible for the Army social media program. The Army Social Media Guide explains standard operating procedures for official external presences. **The Army Social Media Guide is located at https://www.army.mil/socialmedia**. OCPA Digital Media Division will—

- Approve all official social media sites for registration with the Army social media directory at

https://www.army.mil/socialmedia/directory.

Commanders will—

(1) Provide authorization to establish official social media accounts in compliance with local network restrictions.

(2) Authorize social media managers to release information on the command's behalf.

(3) Ensure that social media managers are properly trained and certified and follow guidelines outlined within this regulation.

(4) Ensure social media manager has the proper equipment and network access to conduct social media operations.

PAOs for ACOMs, ASCCs, DRUs, or their designated representatives will—

(1) Ensure approved social media sites within their command operate within the guidelines in this regulation and provide accurate information to the public.

(2) Ensure social media platforms are registered in the Army social media directory.

(3) Maintain a roster and network of all social media managers within the command.

Social media managers will—

(1) Manage accounts using only authorized Government equipment and devices.

(2) Ensure approved social media sites within their command operate within the guidelines in this regulation and are compliant with stated policies.

(3) Update content regularly and consistently, ensuring all content and engagement appropriately reflects the command.

(4) Publish properly reviewed, released, and public domain information and imagery. Unreleased or for official use only (FOUO) content is not authorized for release.

(5) Actively engage the public through timely and accurate information sharing while maintaining security and privacy.

(6) Archive and close inactive or noncompliant accounts.

(7) Develop and update local standard operating procedures for social media management and will ensure that efficient operations continue during personnel transitions. Treat social media access and passwords with as much care as PII.

(8) Maintain a continuity book or file for approved social media sites used in support of the brigade or installation mission. Continuity should include:

(a) A roster of all authorized social media accounts and a contact roster of social media administrators within their command.

(b) Social media processes and strategy, to include a public defacement response plan along with a short justification on how the platform meets the needs of the office.

(c) Appointment letters for each approved unit's social media manager(s).

(9) Ensure appointment letters and social media sites are reviewed annually to ensure compliance.

(10) Ensure social media platforms are registered in the Army social media directory.

(11) Review content for OPSEC before publication.

Training. Personnel who manage and release information on official Army social media platforms must be OPSEC level II certified, and be current with required social media training.

Registration. The social media directory registers official social media accounts of organizations with a 1035 civilian or 46 series military occupational specialty with release authority that is OPSEC level II trained and fulfills all training required of social media managers. The Army social media directory is located at https://www.army.mil/socialmedia/directory. Pages must be open to the public. Private groups, accounts, or feeds will not be registered on the U.S. Army's social media directory.

Release authority. Social media managers on official Army social media accounts must be granted release authority by the commanding officer. The authority to manage and release information must be renewed during command and personnel changes.

d. Disclaimers and settings. Army social media platforms must adhere to the following requirements:

(1) Labeled as an official account.

(2) Classified as a Government organization.

(3) User terms of agreement must include:

(a) General disclaimer.

(b) Privacy and security disclaimers.

(c) Copyright and trademark disclaimers.

(d) Moderated account disclaimer.

(e) FOIA notice.

(f) Specific wording, which can be found at the General Services Administration's Negotiated Terms of Service located at **https://www.digital.gov/resources/negotiated-terms-of-service-agreements/**.

(g) **Contact information, which must be a valid .mil or .gov utility email address**.

(h) Official uniform resource locator.

Social media content. Organizations will have a list of communication priorities as a basis for items that should be posted, as well as a working list of topics that should be avoided, perhaps due to sensitivity or controversial issues. These lists are determined by the commander's priorities and the public's needs.

Inappropriate material and prohibitions. The following items are inappropriate for social media sites:

(1) Inappropriate links. Army public sites will not link to offensive or unrelated commercial material.

(2) Personnel security. Army social media sites will not post references to any information that would reveal sensitive movements of military assets or personnel or the locations of units, installations, or personnel where uncertainty is an element of security of a military plan or program.

(3) Operational security and information security. All content on an Army public social media site must be cleared for public release. Do not include material that is classified or FOUO. Do not include scientific and technical information that has not been cleared for public release.

(4) Personal information. Use of personal information protected by the Privacy Act (see AR 25–22) is prohibited.

(5) Copyright information. Copyrighted material may only be used with written permission from the owner (see AR 27–60). U.S. laws on copyright, primarily 17 USC Chapter 1, preserve for the owner of copyrighted material, the benefits and earnings to be derived from the reproduction and distribution of such works. Material that is subject to copyright protection includes "original works of authorship fixed in any tangible medium…," (17 USC 102(a)). It is now accepted that computer software and sequences of code and instructions are subject to copyright. Per 17 USC 105, Government works are not copyright protected.

(6) Political activity. Official Army social media platforms will not engage in political conversations and will not show any form of endorsement such as a share, like, or other reaction to political statements, posts, graphics, or other types of content.

(7) Comments. Social media managers will never post or make comments that are graphic, obscene, explicit, racial, abusive, hateful, vindictive, or intended to defame anyone or any organization.

(8) Legal. Social media managers will not post details about an ongoing investigation or legal or administrative proceeding.

Family Readiness Group pages. Unit FRG pages must adhere to DoD and Army requirements even if they do not qualify to be in the social media directory. FRG pages can be set as open or closed groups, however, they must not exclude any member of the FRG's parent unit. Content created or shared through FRG sites must be approved by the unit's release authority.

Recruiting pages. Pages created and managed by U.S. Army recruiters and their commands represent the U.S. Army and are considered official pages. Therefore, those sites must abide by the same standards of conduct outlined in this chapter. It is the unit commander's responsibility to enforce these policies and refine their digital footprint.

Private social media presences on third party platforms. Official government use of private or closed social media groups are not authorized. Nonpublic information may not be released outside of the DoD network to include discussions on third party platforms. Doing so would constitute an unauthorized release of nonpublic information per 5 CFR 2635.703. If an organization is interested in hosting an official closed group, the group should be hosted behind firewall on a DoD approved network such as milSuite or Intelink.

Security and password management. Access to official social media accounts will be carefully managed and included in unit standard operating procedures. Security settings will be maximized and include a two-step verification, if available, by the platform.

Live streaming. All live streamed events should be constantly manned with a contingency plan to take them offline in the event of violence, crime, or imagery unsuited for public consumption.

Content boosting and advertising. Units and social media managers are not authorized to use funds to advertise or boost content.

Archiving. Per guidance from National Archives Item A1, Section A, Part II of Office of Management and Budget Memorandum M–12–18, electronic messages created or received in the course of Army official business on social media platforms are federal records. Electronic messages must be scheduled for disposition. Army imagery used in social media platforms is considered a permanent, released DoD record. Social media managers will develop processes and procedures for regular archiving of content and all VI will be archived in accordance with paragraph 3–4 of this regulation.

Nonaccredited social media accounts

Social media accounts are considered nonaccredited if the organization is not brigade level or above, is not open to the general public, or does not meet the guidance outlined in paragraphs 8–3a through 8–3c. Nonaccredited social media accounts are required to be compliant with the guidelines outlined in this chapter.

Personal use of social media and appropriate online conduct

The U.S. Army views personal websites and social media positively, and it respects the right of Soldiers to use them as a medium of self-expression. However, all Army personnel have limitations on what they can discuss. In addition to specific ethics and Hatch Act limitations, civilians are prohibited from

discussing the intricacies of the Army and the DoD. Soldiers on active duty must abide by certain restrictions to ensure good order and discipline. All Soldiers are on duty 24 hours a day, 365 days a year, and their actions are subject to the Uniform Code of Military Justice. Soldiers should also remember OPSEC when posting information in the digital environment.

a. Soldiers are free to further release and share publicly released DoD and DA unclassified information on their personal social media accounts provided no laws or regulations are violated.

b. Soldiers should use their best judgment, remembering that there are always consequences to what is written or photographed. If they are about to post something that is questionable and may reflect negatively on the Army, they should review this and other relevant guidance thoroughly.

c. If still unsure, and the post is about the Army, they should discuss the proposed post with their supervisor or the PA office. Ultimately, however, Soldiers are solely responsible for what they post.

d. Do not post any defamatory, libelous, vulgar, obscene, abusive, profane, threatening, hateful, racially, ethnically, or otherwise offensive or illegal information or material.

e. Do not post any information or other material protected by copyright without the permission of the copyright owner.

f. Do not use any words, logos, or other marks that would infringe upon the trademark, service mark, certification mark, or other intellectual property rights of the owners of such marks without the permission of such owners.

g. Do not post any information that would infringe upon the proprietary, privacy, or personal rights of others.

h. Do not post any nonpublic information (as defined in 5 CFR 2635.703) this includes, but is not limited to, classified or sensitive information, unless such release is a protected disclosure per an appropriate whistleblower statute.

i. Do not forge or otherwise manipulate identifiers in posts in an attempt to disguise, impersonate, or otherwise misrepresent their identity or affiliation with any other person or entity.

j. Soldiers cannot use their service affiliation for fundraising purposes on personal social media accounts except for approved fundraisers such as CFC and the Army Emergency Relief.

k. Soldiers should not use Government email accounts to establish personal accounts.

l. Soldiers cannot invite other Government employees to participate on social media accounts via a Government email address.

m. Employees should not use their official position on personal accounts unless it is accompanied by biographical facts including official photos.

n. All political activity on personal pages must be in compliance with the guidance provided by the Office of The Judge Advocate General.