Corporation for National and Community Service
Policies and Procedures

Policy Number: 105 **Effective Date:** March 8, 2019
Subject: Social Media Policy

Purpose: This policy governs the official use of social media at the Corporation for National and Community Service (CNCS).

Scope and Applicability: This policy applies to all CNCS employees, contractors, interns, and volunteers. Some of the requirements apply specifically to agency users who engage in social media on behalf of CNCS as part of their official duties, whether such use occurs on a CNCS website (intranet or internet), mobile application, or a third-party website.

How will this policy be socialized? This policy will be distributed by email to all personnel and posted on SharePoint. Each CNCS program or office director is included on the clearance sheet for this policy, and is responsible for ensuring that all personnel understand and comply with this policy. External Affairs staff are available to brief others on this policy.

Policy Replaced: Previous versions

Originating Office: Office of External Affairs (OEA)

Approved By:

DESIREE TUCKER-SORINI

Digitally signed by DESIREE TUCKER-SORINI
DN: c=US, o=U.S. Government, ou=Corporation for National and Community Service, cn=DESIREE TUCKER-SORINI, 0.9.2342.19200300.100.1.1=95771003567085
Date: 2019.03.08 09:07:35 -05'00'

Desiree Tucker-Sorini
Chief of Staff

Contents

1. PURPOSE

CNCS is committed to expanding the conversation on national service and upholding the open government principles of transparency, participation, and collaboration. CNCS believes social media can be a significant tool in accomplishing its mission, engaging the public in discussion on issues about national service, and obtaining public input for agency operations.

For purposes of this policy, social media is a broad term for the wide spectrum of interactive and user-driven content technologies (e.g., social networks, blogs, wikis, social bookmarking, video sharing, etc.) that connect users and allow them to engage in dialogue, share information, collaborate, and interact.

The Office of External Affairs (OEA) leads CNCS's social media efforts and works closely with the Office of General Counsel (OGC) and the Office of Information Technology (OIT).

The purpose of this document is to establish policy and procedures for how CNCS staff uses social media.

2. SCOPE AND APPLICABILITY

This policy applies to CNCS employees, contractors, interns, and volunteers (agency users). Specific policy requirements also apply to agency users who produce social media content or engage in social media on behalf of CNCS as part of their official duties.

The Standards of Ethical Conduct (5 C.F.R. Part 2635) apply to an individual's *personal* and *official* use of social media, and this policy does not modify those legal responsibilities. The Hatch Act (5 U.S.C. §§ 7321-7326) limits certain political activities of most executive branch employees, including certain activities on social media.

3. VISION AND STRATEGY

CNCS's mission is to improve lives, strengthen communities, and foster civic engagement through service and volunteering. OEA communicates this mission online to develop and foster relationships with the public, currently-serving national service participants, alumni, external stakeholders, and national service champions.

OEA mobilizes individuals, organizations, and communities through CNCS's mission, programs, special events, and initiatives. Social media is integral to this effort because it provides a platform for real-time conversation, collaboration, and idea sharing. CNCS uses social media to foster a more effective and transparent government and to engage the agency with the public and national service community.

4. POLICY

a) CNCS Social Media Policy

It is CNCS's policy to use social media when:

- OEA has identified a need to engage with the public
- Procedures for establishing a CNCS social media presence have been followed
- The benefits of using the medium outweigh any costs or risks.

CNCS will only use social media sites that have been approved according to CNCS procedures (see 4(b) below) and only when use of the social media site has been approved by the Director of External Affairs. All use of social media must be in accordance with approved Terms of Service (ToS) agreements. OGC must review and approve ToS agreements. OEA will maintain all approved ToS agreements involving third-party websites.

Agency users who manage or use CNCS social media in their official capacity, and the agency's use of social media as a whole, must follow all applicable laws, regulations, and policies regarding, but not limited to, managing personally identifiable information (PII) and CNCS information. Each CNCS social media account requires an account point of contact and designated alternate, who must be CNCS employees. These include, but are not limited to: records management, Section 508 of the Rehabilitation Act on access for persons with disabilities, privacy, ethics, copyright, and information security.

b) Process to Establish a New Official CNCS Social Media Account

OEA directs all social media activity for the agency. OEA will make final decisions about new accounts and will help as needed with implementation and compliance.

If you would like to initiate a new social media account for your program or office, send your request to socialmedia@cns.gov. Include a justification for the account, a point of contact and alternate, and a content strategy. The content strategy must include an outline of topics that will be amplified during the first 90 days. After the new account has been in use for 90 days, report account analytics within 10 business days. OEA will give all account owners and alternates written guidance on posting content, moderating comments, and posting appropriate disclaimers.

Any accounts which are not approved in advance by OEA will be considered private and will be removed from a CNCS website. Any activity that takes place on these accounts will not be considered official use and must therefore comply with the requirements that apply to private social media accounts, which are summarized in Section 7 of this policy.

If you would like to use new social media software, services, access, or tools, also send your request to socialmedia@cns.gov for OEA review. If you are interested in a social media tool or application that is not part of CNCS's portfolio, but is offered by digitalgov.gov, use the social media request form to ask for a CNCS ToS agreement. Include a justification for use with the request. OGC, OEA, and OIT will review ToS agreements before OEA grants official use. The ToS process takes from four to six weeks to complete.

OEA will coordinate with OGC to review current social media accounts to ensure consistency of

messaging and compliance with laws, regulations, and this policy. CNCS may close down social media accounts that do not meet these requirements. In addition, the agency will deactivate accounts if the POC or alternate POC has not completed the required agency training conducted by OEA twice a year. OEA will work with program and/or office supervisors to determine appropriate next steps to remedy non-compliance with policy, law, or regulation.

Any CNCS employee who has a highly visible, publicly-facing position at CNCS, such as a senior director, senior political appointee, or senior discretionary appointee, may only use CNCS official email or social media accounts to post or share national service news, initiatives, programs, and other related content, and to share or retweet official CNCS social media postings. Such employees may not use CNCS official accounts for any personal use, such as sharing or retweeting personal views or opinions.

For purposes of this policy, a CNCS senior director or senior political appointee is defined as a person who receives a salary within the NX-2 pay band and whose position description includes authorization to speak on behalf of the government, including engaging with public and the media.

5. ROLES AND RESPONSIBILITIES

Personnel in multiple offices and programs play a significant role in establishing and monitoring compliance with social media policy. Together they protect CNCS's security and ensure the agency's compliance with all applicable laws and regulations.

a) The Office of External Affairs (OEA):

- Leads CNCS into new social media platforms and uses and drives innovation and online communication via social media
- Manages CNCS's online brand
- Monitors agency users' compliance with this policy
- Oversees social media communications and content and interfaces with programs and state offices accordingly
- Approves all social media accounts
- Serves as the primary contact for any third-party social media companies and social media business
- Coordinates the implementation of ToS agreements with sites in consultation with OGC and OIT
- Develops and implements biannual social media awareness training for people covered by this policy, and provides ad-hoc training for new employees.

b) Programs (AmeriCorps State and National, AmeriCorps NCCC headquarters and campuses, AmeriCorps VISTA, Senior Corps):

- Provide assistance and resources in coordination with OEA
- Participate in weekly meetings to disseminate information and receive updates and training

- Provide new account requests to OEA
- Collaborate with OEA through their account manager(s) and designated alternate account manager(s) to ensure compliance with this policy.

c) Account Manager (and Designated Alternate Account Manager):

- Oversees day-to-day management of the official CNCS social media platform(s) for which the account manager is responsible
- Generates and approves content for the social media platform(s), and moderates comments and activity on page(s) as necessary
- Manages records for their account
- Ensures all branding and style guide requirements are followed
- Participates in required OEA meetings for social media account managers.

d) The Office of Field Liaison (OFL):

- Provides assistance and resources to state offices in coordination with OEA
- Participates in meetings to disseminate information and receive updates and training
- Sends new state office account requests to OEA
- Collaborates with OEA through its account manager(s) and designated back-up manager(s) to ensure compliance with this policy.

e) The Office of General Counsel (OGC):

- Provides legal advice and guidance on social media platforms and the use of social media
- Participates in trainings to inform new account managers and alternate account managers on PII, FOIA, and other issues that affect the use of social media
- Reviews and amends ToS agreements when appropriate
- Oversees ethics requirements for CNCS employees, including advising on proper use of social media in a CNCS employee's personal capacity.

f) The Office of Information Technology (OIT):

- Reviews all new social media technologies, applications, or services submitted by OEA to ensure compliance with IT requirements (e.g., Security/Section 508) and ensure compatibility with CNCS's technical environment
- Works with OEA to conduct security analysis on all new ToS requests.

6. OFFICIAL USE OF SOCIAL MEDIA

Official use is different from an agency user's personal use. When an agency user communicates in an official capacity, he or she is communicating on behalf of CNCS, comparable to standing at a podium at a conference, communicating the agency's views to the audience.

a) Contribution to CNCS Social Media Accounts

CNCS's social media accounts help advance the agency's mission. Programs and state offices are encouraged to submit content to OEA daily. Employees can contribute content to CNCS's core accounts—including platforms such as Twitter, Facebook, Instagram, Tumblr, and YouTube by emailing socialmedia@cns.gov with the proposed content, the requested platform, and a brief explanation of the need or benefit of the outreach.

b) Privacy Requirements

Various laws, including the Privacy Act of 1974, as amended and the Office of Management and Budget policies on third party sites and multi-session cookies, require federal agencies to have policies in place for the protection of individual privacy and PII. Agency users must properly safeguard confidential, privileged, classified, privacy-protected and/or CNCS information. They must also must comply with the standards of employee conduct and the CNCS Privacy Policy, which prohibits disclosure of information learned in the course of the work performed at the agency.

The legal requirements, and CNCS's implementation of the requirements pertaining to the protection of CNCS information, individual privacy, and PII, can be found at CNCS's implementing regulations at 45 CFR Part 2508 and CNCS Policy 153, Privacy Policy.

c) Nonpublic Information

An employee may not disclose non-public information. Non-public information may include, but is not limited to information that is (1) routinely exempt from disclosure under 5 U.S.C. 552 or otherwise protected from disclosure by statute, Executive Order, or regulation; (2) is designated as confidential by an agency; or (3) has not actually been disseminated to the general public and is not authorized to be made available to the public on request.

d) Freedom of Information Act Requirements

The Freedom of Information Act (FOIA) provides a right of access to specific federal agency records. Voluntary disclosure of information through a social media platform outside the federal government may waive the application of statutory exemptions under federal law and compromise CNCS's ability to withhold such information in the future. If you have concerns about making information publicly available through social media or questions regarding the Freedom of Information Act, contact CNCS's FOIA/Privacy Act Officer by phone at 202-606-6747 or by email at FOIA@cns.gov.

e) Section 508 (Accessibility) Compliance

Section 508 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 794(d)), requires that federal agencies' electronic platforms are accessible to people with disabilities. Content posted on social media must be Section 508 compliant.

f) Comment Policy and Moderation

CNCS fosters conversation on its social media platforms and respects the diversity of opinions expressed there. CNCS does not pre-screen or moderate user comments, and user comments are

automatically posted. However, they may be removed by an account manager if they violate CNCS's comment policy (see below). It is the account manager/alternate's responsibility to review comments as soon as possible—preferably within two hours of posting.

All users have a responsibility to maintain an appropriate level of professional conduct in the workplace, and to treat fellow employees with respect and fairness. CNCS Policy 206, Anti-Harassment Policy and Procedures, prohibits harassing conduct (sexual or non-sexual) in any CNCS workplace or in any work-related situation at any other location, both during or outside normal duty hours. CNCS also prohibits retaliation against an employee who alleges harassment, as already defined above, or who assists in any inquiry related to allegations of harassment.

All CNCS social media accounts must post the following comment policy:

CNCS encourages discussion and comments. Your insights help ensure the public is informed and can be a part of CNCS's work every day. Participants are expected to show respect, civility, and consideration to the authors and site visitors, who may include children. To that end, we reserve the discretion to remove a comment if it

- *Contains obscene, indecent, vulgar, abusive, or profane language or material*
- *Contains threats or personal attacks of any kind*
- *Contains hate speech or any discriminatory remark about race, color, sex, sexual orientation, national origin, ethnicity, age, religion, or disability*
- *Is clearly off-topic or spam*
- *Contains sensitive, confidential, or personally identifiable information*
- *Promotes or endorses specific commercial services, entities, or products*
- *Contains defamatory statements*
- *Contains offensive terms targeting individuals or groups*
- *Suggests or encourages illegal activity*
- *Supports the passage or defeat of legislation before the Congress or any state or local legislative body*
- *Advocates or promotes any proposed, pending, or future federal, state, or local tax increase*
- *Advocates any proposed, pending, or future requirement or restriction on any legal consumer product*
- *Contains unsolicited proposals or other business ideas or inquiries, or any other comments deemed inappropriate.*

If your comment contains objectionable or inappropriate content, it may be deleted. Comments will not be edited. To protect your privacy and the privacy of others, please do not include your or others' full name, phone numbers, email addresses, Social Security Numbers, case numbers, or any other sensitive or personally identifiable information (PII) in your comments or responses. The views expressed in the comments only reflect those of the comment's author, and do not necessarily reflect the official views of the agency, or the federal government. Under the Children's Online Privacy Protection Act of 1998, persons under the age of 13 are not allowed to submit questions or comments. Comment review will occur during normal business hours. Please ensure that your comments comply with this policy.

g) Information Collection and Paperwork Reduction Act

The Paperwork Reduction Act (PRA) covers the collection of data from the public. The PRA requires OMB approval of all surveys or other information collections given to ten (10) or more participants. This includes any sort of survey where identical questions are given to ten or more participants, regardless of the format. One exception to this requirement is when an agency uses an anonymous submission form and users can provide open ended comments or suggestions without any government guidance on the content.

CNCS's information collection guidelines can be found in the Clearing Information Collection Requests policy. Questions about the applicability of the PRA should be directed to the Office of General Counsel or the Associate Director for Policy.

h) Lobbying and Propaganda

Federal requirements under 18 U.S.C. §1913 and provisions in federal appropriations acts prohibit the use of appropriated funds to lobby members of Congress. This includes "grassroots lobbying"—appealing to members of the public to contact their elected representatives in support of or opposition to legislative matters or proposals.

"Use of appropriated funds" extends to the payment of employee salaries, equipment, office space, etc. Such funds may not be "used directly or indirectly to pay for any personal service, advertisement, telegram, telephone, letter, printed or written matter, or other device, intended or designed to influence in any manner a Member of Congress, to favor or oppose, by vote or otherwise, any legislation or appropriation by Congress, whether before or after the introduction of any bill or resolution proposing such legislation or appropriation..."

Federal employees using social media should be mindful of 18 U.S.C. § 1913, because a violation or attempt to violate the statute may result in a fine, imprisonment, or removal from government office or employment.

All CNCS-authored social media posts must identify CNCS as the source. In December 2015, the U.S. Government Accountability Office (GAO) issued a finding that a federal agency violated publicity or propaganda and anti-lobbying provisions contained in appropriations acts with its use of certain social media platforms in association with one of the agency's rulemaking actions, B-326944 (Dec. 14, 2015). The provisions discussed in that decision are applicable to CNCS. Employees of CNCS are prohibited from requesting that social media users post a government-authored message to their social media networks, unless the message expressly attributes, or it is expressly apparent that, CNCS is the source of the message.

i) Records Management

All CNCS-generated content is subject to the requirements of 44 U.S.C. Chapter 31 – Records Management by Federal Agencies. Federal records in social media platforms include:

- Social media content records, including entries, comments, blog posts, links, videos, and other social media communications

- Social media site management and operations records, including design, policy and procedures, and other social media management records.

To ensure compliance with NARA Bulletin 2014-02, Guidance on Managing Social Media Records, account managers are responsible for managing records, as defined above, complying with CNCS Policy 506 on Records Management, and monitoring any changes to ToS agreements that may affect records management.

j) Prohibitions on Engaging with CNCS Personal Social Media Accounts

Official CNCS social media accounts are prohibited from engaging with the personal social media accounts of CNCS employees. This prohibition includes tagging, liking, sharing, commenting, re-tweeting, and quote-tweeting. The prohibition is designed to avoid creating the perception of CNCS endorsement of any employee's personal views.

If employees wish to contribute to the agency's existing social media accounts, they should submit content to socialmedia@cns.gov in accordance with section 6(a) above. Employees are required to use working hours to perform official duties. Use of CNCS computer systems, including all mobile and electronic devices, is subject to CNCS Cybersecurity User Rules of Behavior (ROB) and restrictions on use which employees sign each year.

Employees are subject to the applicable Standards of Conduct for Employees of the Executive Branch and the Hatch Act (5 U.S.C. 7321-7326) which governs partisan political activity of Executive Branch employees. (The link above is for a summary of the Standards of Conduct. To see the full regulation go to 5 C.F.R. Part 2635.)

Requesting new accounts, managing accounts, or submitting content on OEA social media platforms may trigger the provisions of the Federal Advisory Committee Act (FACA) or of the Paperwork Reduction Act (PRA). OEA will submit these requests to the Associate Director for Policy and OGC for review. CNCS programs are required to work with their legal counsel and with the Associate Director for Policy to ensure that social media content does not trigger the provisions of FACA or the PRA.

k) Copyright and Fair Use

Copyrighted materials must be used in accordance with current copyright laws (Title 17, U.S. Code), which generally requires permission from the copyright owner. However, the doctrine of fair use is a limitation on copyright owners' right to prohibit others from using their copyrighted material. Title 17, Section 107 of the U.S. Code contains a list of purposes for which the reproduction may be considered fair use, as well as a list of factors to consider in making the fair use determination. If a copyright or fair use question arises, individuals must contact OEA and OGC.

l) Information Quality

The public places a high degree of trust in federal agency content and considers it an authoritative source. Under section 515 of Pub. L. No. 106-554, agencies are required to maximize the quality, objectivity, utility, and integrity of information and services provided to the public. With social

media information dissemination products, agencies must reasonably ensure suitable information and service quality that is consistent with the level of importance of the information. Reasonable steps include: 1) clearly identifying the benefits and limitations inherent in the information dissemination product (e.g., possibility of errors, degree of reliability, and validity), and 2) taking reasonable steps to remove the limitations inherent in the product or information produced. Agency management must ensure that this agency position is reflected in all communications rather than any one person's opinion.

m) Availability to Persons with Limited English Proficiency

Executive Order 13166 requires that agencies take reasonable steps to ensure meaningful access to their federally conducted programs and activities by persons with Limited English proficiency (LEP). This was reaffirmed by Attorney General Memorandum: Federal Government's Renewed Commitment to Language Access Obligations under Executive Order 13166, dated February 17, 2011.

The use of social media technologies to communicate and collaborate with citizens is a federally-conducted activity. In order to ensure meaningful access by LEP individuals, agencies must conduct a flexible and fact-dependent individualized assessment that balances four factors:

1) Number or proportion of eligible LEP persons
2) Frequency of contact
3) Nature and importance of the program or activity
4) Availability of resources.

This framework was established by the U.S. Department of Justice (DOJ) to guide federal agencies on the implementation of and compliance with Executive Order 13166. For more information on LEP at CNCS, please contact CNCS's Equal Opportunity Program.

n) Security Requirements and Risk Management

The Federal Chief Information Officer Council's Privacy Best Practices for Social Media outlines recommendations for using social media technologies in a manner that minimizes risk while also embracing the opportunities these technologies provide.

Federal government information systems may be targeted by persistent, pervasive, and aggressive threats. In order to mitigate rapidly evolving social media threats, CNCS will:

- Control official use of social media
- Implement user awareness and training (see section 7 below) and maintain in OEA a list of the employees who have access to CNCS social media accounts and their related training
- Require new employees to sign the CNCS Cybersecurity User Rules of Behavior agreement
- Maintain host and/or network controls
- Secure configuration of social media software to determine overall risk tolerance for use of social media technologies.

In order to maintain appropriate levels of security for account managers of CNCS social media:

- Every person must have a separate password for each account (CNCS recognizes that some

social media platforms, by their very nature, are shared by multiple employees).

- If shared, passwords must be changed when any employee with the password leaves CNCS or is transferred to a position that no longer requires access to the account.
- Employees with access to shared accounts must agree to abide by the rules for using a social media account, as discussed in this policy and at the training identified in paragraph 7 below.
- Employees with access to such accounts may only give access to others once they get OEA's authorization via socialmedia@cns.gov.
- All passwords must be changed every 90 days.
- If an employee is leaving CNCS, the account POC must notify socialmedia@cns.gov no less than 24 hours before departure.
- Upon departure from CNCS, all social media accounts associated with the departing employee must be transferred to authorized CNCS personnel.
- Transferred accounts must have passwords changed immediately upon receipt.

OEA will coordinate with OIT to ensure social media technology complies with current security approvals and the risk management framework.

o) Emergency Use

In the event of an emergency, social media platforms will be used in accordance with the Continuity of Operations Plan, which calls for a coordinated messaging effort between OEA and programs or offices. Under no circumstances should a state, program, or campus account first send out a message about an emergency. Account managers and/or the designated alternate managers must wait for guidance from OEA.

7. Personal Use of Social Media

CNCS employees may not create or use personal accounts or handles to conduct official business. This includes use of CNCS logos or official pictures in the profiles of personal accounts. The only exception regarding CNCS logos is when the social media platform automatically uploads the CNCS logo when you enter your place of employment. However, CNCS does encourage employees—except those employees defined as a senior director, senior political appointee, or senior discretionary employee—to re-tweet, favorite, share, and like official CNCS social media on their personal accounts, so long as the employee follows the guidance below. Employees may contact socialmedia@cns.gov with questions.

Examples of CNCS official business that are not allowed on your personal social media account include, but are not limited to:

- Using social media messaging platforms (for example, Facebook Messenger, Twitter Direct Messages, Instagram Direct) in place of CNCS email
- Responding to comments on behalf of CNCS using your personal account.

Official business ***does not include*** general amplification of national service news, initiatives, and programs, including sharing or retweeting of official CNCS social media.

- If you identify yourself as a CNCS employee in your profile (for example, Facebook Profile, Twitter Profile, Instagram, etc.) it is highly recommended that your CNCS information includes

a disclaimer. If you do not use a disclaimer you may be found to be in violation of misusing your position and/or title, or in violation of the Standards of Conduct for Employees of the Executive Branch.

- An example of a proper disclaimer is "*Views and opinions expressed are my own and do not state or reflect those of the U.S. Government."*
- CNCS employees may not display any CNCS logos, including the AmeriCorps and Senior Corps logos, in their social media profile pictures. This includes Facebook Profile and Cover photos, Twitter Profile and Header photos, Instagram Profile photos, and personal blogs. This includes wearing CNCS, AmeriCorps, or Senior Corps branded uniforms. However, as stated above, logos that are automatically uploaded by the social media platform when you enter your place of employment are allowed in your profile.
- Although CNCS logos and uniforms may not be displayed in profile pictures, they can be displayed on social media posts such as a tweet, Facebook photo, or Instagram photo. Posts that contain CNCS logos or uniforms must avoid the appearance of speaking on behalf of the agency in your official position. Posts must not imply CNCS endorsement or sanctioning of personal opinions.

We encourage personnel to review the FAQs attached to this policy. More information is in the Office of Government Ethics' Legal Advisory (LA-15-03) titled "The Standards of Conduct as Applied to Personal Social Media Use" and the Office of Special Counsel's "Hatch Act Guidance on Social Media." Senior directors, senior political appointees, and senior discretionary appointees who speak or write on current political events or current policy issues in their personal capacity must have prior written approval from the White House Office of Communication and have their comments or writings reviewed by the CNCS Designated Agency Ethics Official (DAEO) before participating in each activity.

If employees have questions regarding acceptable personal use or what constitutes official use, they are encouraged to discuss these questions with OEA and OGC.

8. Communications and Training

The Director of External Affairs will publish this policy on the CNCS intranet. OEA will conduct training with program departments, offices, and individuals that are using social media to communicate on behalf of CNCS, to educate agency users on compliance with this policy.

OEA will also meet with those responsible for supervising contractor performance to ensure compliance with this policy.

All account managers and designated alternate managers will be required to sign an agreement that they have read and understand this policy.

Finally, OEA will work with the Office of Human Capital to implement a learning management system course for all CNCS employees to complete annually.

9. Additional Information

Please contact OEA at socialmedia@cns.gov with any questions about this policy

10. Authority

- OMB Memorandum M-09-12, President's Memorandum on Transparency and Open Government – Interagency Collaboration. February 26, 2009
- OMB Memorandum M-10-06, Open Government Directive. December 8, 2009
- OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications. June 25, 2010
- Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies, Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act. April 7, 2010
- Corporation for National and Community Service, "Open Government Plan," released April 7, 2010.

11. Related Documents

- Information Technology Management Reform Act of 1996 (absorbed under Clinger-Cohen Act of 1996) (40 U.S.C. § 1401)
- Records Management by Federal Agencies (44 U.S.C. Chapter 31)
- Section 508 of the Rehabilitation Act (29 U.S.C. § 794(d)), as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (August 7, 1998)
- Privacy Act of 1974 (5 U.S.C. § 552(a))
- Paperwork Reduction Act of 1980, as amended; Paperwork Reduction Reauthorization Act of 1995 (44 U.S.C. Chapter 35)
- Presidential Memorandum, Managing Government Records. November 28, 2011
- Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. Part 2635
- OMB Memorandum M-13-10, Antideficiency Act Implications of Certain Online Terms of Service Agreements. April 4, 2013
- The Hatch Act, 5 U.S.C. §§ 7321-7326
- The Freedom of Information Act, 5 U.S.C. § 552
- Federal Advisory Committee Act 5 U.S.C. app. as amended
- Political Activities of Federal Employees, 5 CFR part 734
- Copyright Law, 17 U.S.C. Ch. 1-13
- OMB Memorandum M-10-22: Guidance for Online Use of Web Measurement and Customization Technologies. June 25, 2010
- National Archives and Records Administration (NARA) Bulletin 2014-02, Guidance on Managing Social Media Records. October 25, 2013
- Office of Special Counsel, The Hatch Act FAQs on Federal Employees and Use of Social Media
- U.S. Office of Government Ethics, LA-15-03, The Standards of Conduct as Applied to Personal Social Media Use. April 9, 2015
- CNCS FOIA Guidance and Procedures
- CNCS Producing Public Documents: Print and Digital Policy, No 104
- CNCS Cybersecurity Policy, No 376

12. Definitions

Electronic messages are "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals" (44 U.S.C. § 2911(c)(1)).

Non-official/personal use: personal day-to-day use of social media sites by agency users that is unrelated to their official duties.

Official use: social media engagement on behalf of the agency, and as authorized by the agency, on sites where CNCS has an official web presence and a Terms of Service agreement.

Personnel: all CNCS employees, contractors, interns, members, and volunteers

Social media: tools and technologies that allow an agency user to share communications, postings or information, or participate in social networking, including but not limited to: blogs (such as Twitter or Tumblr), social networks (such as Facebook, LinkedIn, Google+), video and photo sharing websites (such as Instagram, Flickr), online forums and discussion boards (including commenting online using media websites), and automated data feeds. "Social media" does not include non-public tools and technologies, such as CNCS's internal SharePoint site.

Attachment: Personal Social Media Use FAQs

Corporation for National and Community Service
January 2019

At CNCS, we understand that social media use is complex and ever-changing. These FAQs are meant as a companion to the agency's official social media policy. While this list does not cover every use of every social media platform, we hope that it provides general guidance on navigating personal social media as a federal employee.

This is a living document that will continue to be updated. If you have any specific questions, please contact the CNCS's Designated Agency Ethics Official.

As an employee, it is your responsibility to ensure that your personal social media accounts are in compliance as of the effective date on the CNCS Social Media Policy (12/15/2017) or your date of employment, whichever is most recent.

1) May I identify as a CNCS employee on my social media accounts?

Yes, as CNCS staff you have the option to identify yourself as a CNCS employee in your profile, but you cannot conduct official business or set up your account and posts in a way that implies you are speaking on behalf of the agency in your official position. Additionally, you may include your title or position as one of several profile details when such information is given to identify you, provided that it is not given more prominence than other significant profile details.

2) I don't identify as a CNCS employee on my personal social media. Does the social media policy still apply to me?

There are sections of the social media policy and these FAQs still apply to you. Notably, the Hatch Act and the prohibition on conducting official business from your personal accounts applies whether or not you identify as a CNCS employee online.

If you do not identify as an employee, you do not need to place a disclaimer on your social media profile. However, if your followers know you are a CNCS employee and you are discussing CNCS in any way, we recommend you place a disclaimer on your account.

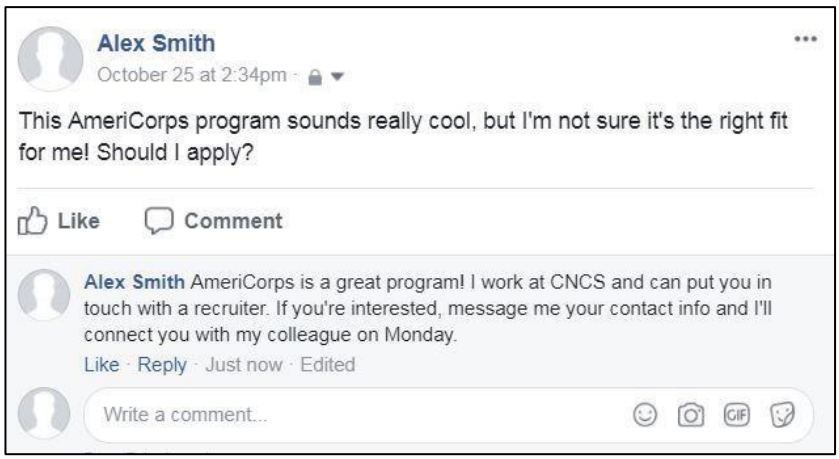
3) What do you mean by "official business?"

Official business includes, but is not limited to:

- Disclosing non-public information that you are privy to as a CNCS employee
- Using social media messaging platforms like Facebook Messenger, Twitter Direct Messages, and Instagram Direct in place of CNCS email for business communications
- Responding to comments using your personal account in a way that speaks on behalf of the agency in your official capacity.

At the first opportunity, you should direct CNCS inquires to official CNCS platforms and mailboxes. See the examples below on how you should transition as quickly as possible from social media comments and messages to official CNCS email to conduct government business. For comments and inquiries posted on official CNCS accounts, all official CNCS account holders should respond as the official account rather than as their personal account.

Appropriate use:



Inappropriate use:

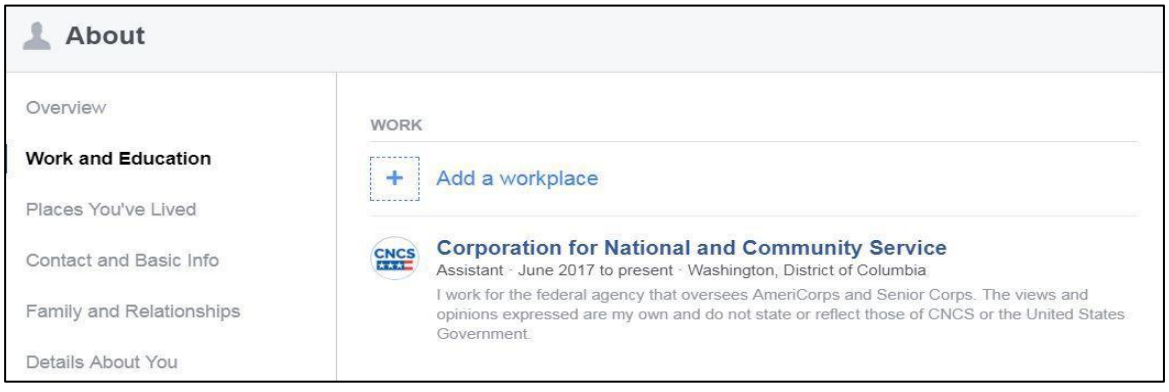
4) I identify as a CNCS employee on my personal social media. How do I show that these are my personal views and not those of the agency?

We highly recommend that all employees identifying as CNCS staff on social media put a disclaimer in their profile stating that "*All views and opinions expressed are my own and do not state or reflect those the U.S. Government."*

<u>Examples:</u>

Facebook Profile:

Copy and paste the disclaimer in the section of your profile that mentions your CNCS employment.



Twitter Profile:
Add an abbreviated version of the disclaimer for character limits:
“Tweets are my own & don’t reflect CNCS.”

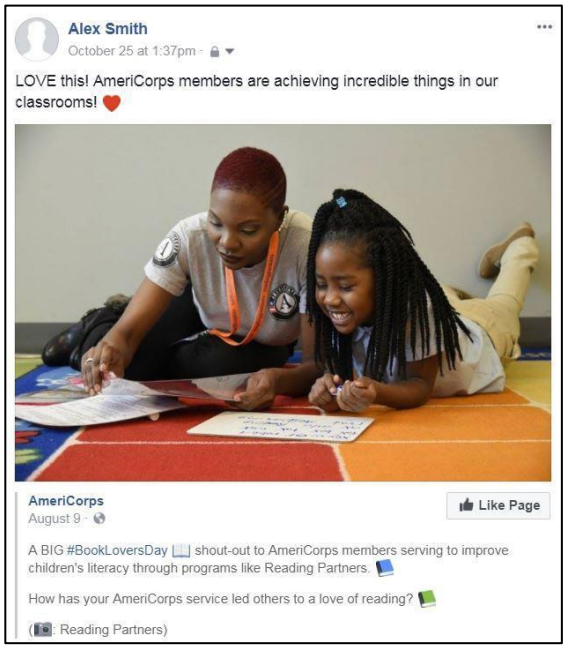
5) May I retweet, share Facebook posts, or promote other official CNCS messages on my personal account?

Yes, you can certainly share the public messaging of CNCS on your social media accounts.

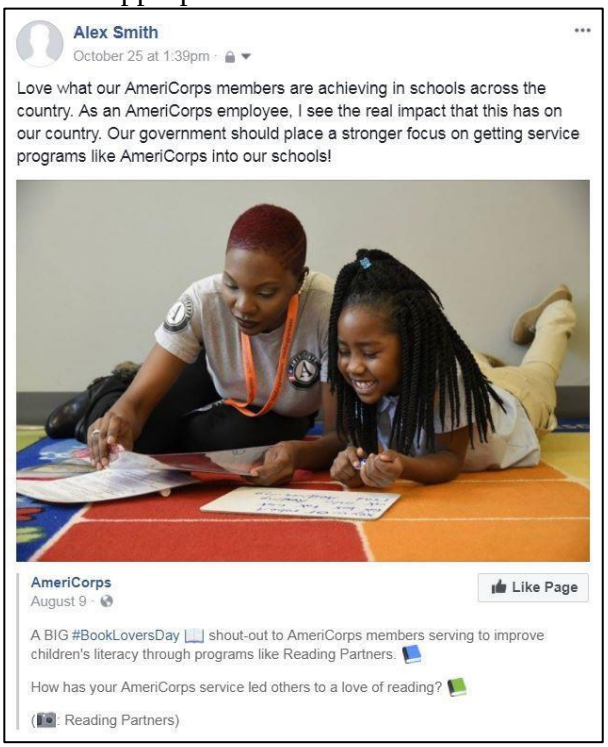
There is nothing wrong with retweeting Senior Corps or sharing an AmeriCorps Facebook post. The only exception are those employees described in the Social Media Policy section 4b.

It becomes an issue when you editorialize the content while confirming your position as a CNCS employee in a way that appears to speak on behalf of the agency.

Appropriate Post:



Inappropriate Post:



The key difference between these two statements is that, in the Inappropriate Post, Alex identifies as a CNCS employee while advocating an opinion related to the agency. It can be reasonably perceived that Alex is commenting under an official government capacity of CNCS in this post.

6) May I share online content created by external outlets that discusses CNCS programs, initiatives, and/or funding?

Yes, you may share external content about national service, including news articles and blogs, as long as you do not editorialize the content while confirming your position as a CNCS employee in a way that appears to speak on behalf of the agency.
Note: For questions regarding partisan political content, please see the Hatch Act section below (Questions 11-13).

7) May I display any CNCS, AmeriCorps, or Senior Corps logos, uniforms, or gear in my social media profile pictures?

No. CNCS employees may not display any CNCS logos, including the AmeriCorps or Senior Corps logos, in their social media profile pictures. This includes Facebook Profile and Cover photos, Twitter Profile and Header photos, Instagram Profile photos, and personal blogs profile photos. This includes wearing CNCS, AmeriCorps, or Senior Corps branded uniforms. The only exception regarding CNCS logos in your profile is when the social media platform automatically uploads the CNCS logo when you enter your place of employment.

8) May I display any CNCS, AmeriCorps, or Senior Corps logos, uniforms, or gear in my social media profile pictures during AmeriCorps Week or Senior Corps Week?

No, even during special events and promotions, employees are prohibited from displaying CNCS logos in their profile photos, cover photos, or header photos. We encourage you to find other ways to show your spirit!

9) What about logos that auto-populate? For example, LinkedIn and Facebook automatically use the CNCS logo when I put my place of employment in my profile.

This is a permissible use of logo. Make sure that there is a disclaimer on your profile as outlined above. Additionally, you may include your title or position as one of several profile details when such information is given to identify you, provided that it is not given more prominence than other significant profile details.

10) May I post images of CNCS logos or photos of me in CNCS gear on social media?

If the photos are not in your profile picture and do not imply CNCS endorsement or sanctioning of personal statements and/or opinions, you may post a photo that includes CNCS logos on your social media account. However, when there is a question regarding whether you are using your personal social media account within the bounds of the Executive Branch Standards of Conduct, an ethics official will look at all the facts, including but not limited to your disclaimer, biographical information and the level of CNCS reference compared to other non-CNCS references on your account.

Appropriate Use:

Inappropriate Use:

Hatch Act

11) The policy states that using social media in an official capacity to engage in political activity is a violation of the Hatch Act. Does this include my personal social media if I identify as a CNCS employee in my profile?

You are most likely safe. To violate the Hatch Act, you clearly need to be on duty, in a federal workspace, or otherwise tied to acting in your official capacity. Merely naming where you work in your profile does not meet that standard.

One important exception is sharing, retweeting, or liking social media content that solicits partisan political contributions. As a federal employee, you cannot solicit or fundraise for partisan political contributions at any time or under any circumstance, including social media. So make sure if you are sharing, retweeting, or liking social media content that links to a partisan political party or candidate it is to a page that is not directly soliciting donations.

12) What if I retweet or share content that links to a campaign website on my personal social media?

As a federal employee, you may link to a campaign webpage as long as the linked webpage is *not* the donation page, where you are specifically required to enter your credit/debit card in order to make a donation.

13) What about sharing online content that advocates for or against legislation, like a Congressional budget or President's budget?

If you identify as a CNCS employee on your personal social media, you cannot encourage citizens to lobby for agency funding or legislation in a way that implies you are speaking in your official capacity. Federal employees can never encourage citizens to contact Congress in our official capacity.