UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

# Social Media Policy


**OPM**.GOV

JULY **2017**

# United States Office of Personnel Management
# Social Media Policy
# Version 6.0

## 1.0 PURPOSE AND DEFINITION

The purpose of this document is to detail the policy for the use of social media at the U.S. Office of Personnel Management (OPM) and applies to official use of social media by agency users on behalf of OPM for agency purposes, including citizen engagement, and where indicated, to non-official/personal use of social media by agency users. These two types of social media use are defined as:

1) **Official Use:** Social media engagement on behalf of the agency and as authorized by the agency on sites where OPM has an official web presence and terms of service agreement.
2) **Non-Official/Personal Use:** Personal day-to-day use of social media sites by agency users, not related to official duties.

The purpose of this policy is to provide guidance for OPM employees, non-paid interns and employees of contractors to permit those performing work on behalf of the agency to take full advantage of social media[1] while at the same time protecting the agency and its employees by mitigating risk. Pursuant to current agency disciplinary procedures and policies, misuse of government equipment/resources, non-compliance with or failure to follow agency policy, procedures, and guidance while using social media, or any other actions that violate applicable law or policy may result in disciplinary action for employees and other actions appropriate to their situation for other individuals performing work on behalf of OPM.

For the purposes of this policy, "social media" covers tools and technologies that allow a social media user to share communications, postings or information, or participate in social networking, including but not limited to: blogs (e.g., Twitter, Tumblr), social networks (e.g., Facebook, LinkedIn, Google+), video and photo sharing websites (e.g., Instagram, Flickr), online forums and discussion boards, and automated data feeds.

This purpose of this document is to detail the policy for the use of social media at the U.S. Office of Personnel Management

## 2.0 APPLICABILITY

This policy applies to all U.S. Office of Personnel Management (OPM) employees, non-paid interns and employees of contractors (hereinafter referred to as "agency users"). All agency users are expected to comply with relevant law and policies when utilizing internal and external social media platforms. Pursuant to applicable law, certain sections of this policy apply only to OPM employees, as noted. This policy is effective, as amended on August 16, 2017.

## 3.0 SCOPE

[1] "Social Media" also known as "Web 2.0" or "Gov 2.0" are web-based tools, websites, applications and media that connect users and allow them to engage in dialogue, share information, collaborate, and interact. Social media websites are oriented primarily to create a rich and engaging user experience. In social media, users add value to the content and data online; their interactions with the information (e.g., both collectively and individually) can significantly alter the experiences of subsequent users.

It is the policy of OPM to support the official use of social media to assist users in accomplishing the agency's mission of recruiting, retaining, and honoring a world-class workforce to serve the American people. OPM believes that the appropriate use of social media improves transparency, collaboration, and participation in support of the agency's mission. This policy is designed to aid agency users in understanding and adhering to the proper use and protection of government equipment in conducting social media activities.

OPM must comply with applicable federal laws, regulations, and requirements including, but not limited to, Section 508 of the Rehabilitation Act of 1973, as amended in 1998, privacy, ethics, copyright, information security, and records management in its social media use.

This policy does not apply to the Collection, Use and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications. See Security Executive Agent Directive (SEAD) 5.[2]

OPM use of social media platforms will change over time as technology evolves. These guidelines cover all internally and externally utilized social media platforms including, but not limited, to:

- Social Networking Sites (Facebook, Google+, LinkedIn, etc.)
- Micro-blogging sites (Twitter, Tumblr, etc.)
- Blogs (including OPM official use and non-official/personal use blogs, as well as comments)
- Agency User Posts to THEO
- Video and Photo Sharing Websites (Instagram, YouTube, Flickr, etc.)
- Forums and Discussion Boards (non-official and personal use of Google Groups, Yahoo! Groups)
- XML & RSS Feeds
- Ideation Programs (IdeaScale, IdeaFactory, etc.)
- Online Information Repositories/Encyclopedias for both official use (e.g., Max.gov) and non-official/personal use (e.g., Wikipedia)
- Emerging/new technology identified as social media by GSA's DigitalGov.gov website to help government workers deliver a better customer experience to citizens.

## 4.0 AUTHORITIES

- Acts Affecting a Personal Financial Interest, 18 U.S.C. § 208
- Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR part 2635
- Supplemental Standards of Ethical Conduct for Employees of the Office of Personnel Management, 5 CFR part 4501
- The Hatch Act, 5 U.S.C. §§ 7321-7326
- Political Activities of Federal Employees, 5 CFR part 734
- Records Management by the Archivist of the United States, 44 U.S.C. Ch. 29

[2] Available online at: https://www.dni.gov/files/documents/Newsroom/Press%20Releases/SEAD5-12May2016.pdf

- Records Management by Federal Agencies, 44 U.S.C. Ch. 31
- Records Management, 36 CFR Ch. XII Sub Ch. B
- Disposal of Records, 44 U.S.C. Ch. 33
- Freedom of Information Act, as amended, 5 U.S.C. § 552
- Privacy Act of 1974, as amended, 5 U.S.C. § 552a
- OPM Information Technology Policies
- Paperwork Reduction Act, 44 U.S.C. Ch. 35
- Concealment, Removal or Mutilation of Records, 18 U.S.C. § 2071
- Copyright Law, 17 U.S.C. Ch. 1-13
- Section 508 of the Rehabilitation Act of 1973, as amended in 1998 (29 U.S.C. § 794 (d))
- Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505.
- President Barack Obama, Memorandum on Transparency and Open Government (Jan. 21, 2009). https://www.gpo.gov/fdsys/pkg/FR-2009-01-26/pdf/E9-1777.pdf
- OMB Memorandum M-10-06, Open Government Directive (Dec. 8, 2009).
- OMB Memorandum, Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act (April 7, 2010).
- OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010).
- OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010).
- OMB Memorandum M-13-10: Antideficiency Act Implications of Certain Online Terms of Service Agreements (April 4, 2013).
- 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 (December 18, 2015).
- U.S. Office of Government Ethics: LA-15-03 The Standards of Conduct as Applied to Personal Social Media Use (April 9, 2015).
- GAO Decision, *Environmental Protection Agency--Application of Publicity or Propaganda and Anti-Lobbying Provisions*, B-326944, (Dec. 14, 2015).

## 5.0 ROLES AND RESPONSIBILITIES

### 5.1 – OFFICE OF COMMUNICATIONS (OC)

The OPM Director has delegated to the OC Director the authority to exercise such information sharing and public liaison authorities as may be necessary to carry out assigned functional responsibilities in support of the Director and OPM organizations. In this capacity, OC coordinates a comprehensive effort to inform the public of OPM goals, plans, and activities through various media outlets, including social media.

OC is a co-owner of this social media policy and is responsible for monitoring OPM use of social media sites, referring compliance concerns to appropriate agency personnel and tracking best practices. OC manages the OPM.gov-branded social media accounts. OC also serves as the agency's point of contact for intra-agency

social media working groups. OC oversees OPM program offices' management of program-specific social media accounts for compliance with current agency messaging and strategic communication goals.

**5.2 – CHIEF INFORMATION OFFICER (CIO)**
The CIO is responsible for developing and executing OPM information management activities in conformity with laws, regulations, orders, and directives involving information technology (IT), records management, the Privacy Act, Freedom of Information Act (FOIA), Paperwork Reduction Act (PRA), and other types of information management governance.

As a co-owner of this social media policy, CIO applies the requirements of this policy in its functions of providing appropriate agency-wide web technology services and security, policy, guidance and technical assistance to program offices. Additionally, the CIO (or designee) is responsible for establishing OPM policies, standards, and procedures related to records and information management.

**5.3 – OFFICE OF THE GENERAL COUNSEL (OGC)**
The Office of the General Counsel (OGC) provides legal advice and representation to OPM managers and leaders so they can work to support an effective civilian workforce for the Federal Government. In the context of social media, OGC provides legal guidance relating to the use of third-party and agency sponsored social media, use of the Web, terms of service agreements, ethics requirements for OPM agency users, privacy policies, any other applicable matter and periodically monitors agency-wide social media activities for legal implications.

**5.4 – CHIEF PRIVACY OFFICER (CPO)**
The Chief Privacy Officer (CPO) serves as the principal privacy advisor and is responsible for formulating and implementing OPM policies related to the collection, maintenance, and use of personally identifiable information. In the context of social media, CPO's responsibilities include ensuring compliance with the Privacy Act, the privacy provisions of the E-Government Act, and other privacy-related laws, regulations, and guidance relating to the use of third-party and agency sponsored social media.

**5.5 – WEB AND SOCIAL MEDIA POINTS OF CONTACT**
Web and Social Media Points-of-Contact (POCs) are designated by each Associate Director or Office Head to serve as the primary points of contact for their offices and are accountable for the effective oversight, coordination, and management of information within their respective organizations. As these key POC positions within the program offices will be the first points-of-contact on social media and other web activities, it is imperative that they coordinate closely with their organization's leadership as well as OC, CIO, and OGC. Each will be designated as the social media representative responsible for monitoring his or her program office's compliance with this Social Media Policy and will serve as a contact for any social media responsibilities. POCs generally will also be responsible for posting content to official OPM social media accounts and interacting with the applicable social media accounts' audience in a manner consistent with this policy, OC guidelines, and applicable law, as well as other related guidance. OC, in collaboration with CIO, will provide training to the POCs. Additionally, an internal OPM Web Council, consisting of all Web and Social Media POCs, meets on a monthly basis to share best practices, update information, and to coordinate efforts.

**5.6 – OFFICIAL OPM SOCIAL MEDIA ACCOUNT ADMINISTRATORS**

Official OPM Social Media Account Administrators are designated by OPM program managers to administer and run official OPM social media accounts in a manner consistent with this social media policy, applicable law and related guidance. Administrators are responsible for controlling access to the account and maintaining account security (e.g., secure password maintenance and deactivating account access due to change in staffing).

## 6.0 LEGAL OBLIGATIONS AND RESTRICTIONS FOR SOCIAL MEDIA USE

All OPM agency users are required to comply with the legal obligations and restrictions that apply to online communications at all times, regardless of whether they are at work, outside the office, or using government equipment. The restrictions on OPM employee communications are contained in statutes, the Code of Federal Regulations (CFR) and current agency policies. For example, when using social media tools and third-party sites for either official or personal use, OPM employees are bound by the Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR part 2635 and the Supplemental Standards of Ethical Conduct for Employees of the Office of Personnel Management, 5 CFR. part 4501.

While not exhaustive, the following restrictions apply to all employees, and violations may be cause for disciplinary action by the agency:

- **Criminal or Dishonest Conduct:** Employees shall not engage in criminal or dishonest conduct.

- **Conflict of Interest:** Employees shall not participate in particular matters affecting their own financial interest or the financial interest of other specified persons or organizations. 18 U.S.C. § 208.

- **Misuse of Position:** Employees shall not use their public office for private gain, for the endorsement of any product, service, or enterprise, or for the private gain of friends, relatives, or other acquaintances. Also, employees shall not use or permit the use of their Government position or title or any authority associated with their public office in a manner that is intended to coerce or induce another person to provide any benefit, financial or otherwise, to themselves or to friends, relatives, or persons with whom the employees are affiliated in a nongovernmental capacity. Finally, with limited exceptions,[3] employees shall not use their Government position or title in a manner that could reasonably be construed to imply that the Government endorses or sanctions their personal activities or those of another. 5 C.F.R. § 2635.702.

- **Use of Government Time and Property:** When employees are on duty, the Standards of Ethical Conduct require that they use official time in an honest effort to perform official duties. See 5 C.F.R. § 2635.705. The Standards of Ethical Conduct also require employees to protect and conserve government property and to use government property only to perform official duties, unless they are authorized to use government property for other purposes. See 5 C.F.R. § 2635.704. For example, under the Standards of Ethical Conduct, a supervisor may not order, or even ask, a subordinate to work on the supervisor's personal social media account. Coercing or inducing a subordinate to maintain the supervisor's personal account would amount to a misuse of position and, if done on official time, a

[3] See 5 CFR § 2635.702(b), (c).

misuse of official time. The same would be true if the supervisor were to have a subordinate create content for the supervisor's personal account, even if the subordinate were not involved in uploading the content to that account. 5 C.F.R. §§ 2635.702(a), 2635.705(b). Employees should report such matters to the designated agency ethics officer.

- **Use of Non-Public Information:** Employees shall not allow the improper use of nonpublic information to further their own private interest or that of another, whether by engaging in financial transactions using such information, through advice or recommendation, or by knowing unauthorized disclosure. Non-public information is information that the employee gains by reason of Federal employment and that he or she knows or reasonably should know has not been made available to the general public. 5 C.F.R. § 2635.703.

  Further, employees shall not make careless or intentional unauthorized disclosures of nonpublic information, unless disclosure if authorized by law. Other unauthorized disclosures include, but are not limited to the unauthorized dissemination of classified information, proprietary information, and the content of confidential and deliberative discussions.

- **Political Activity:** Employees must avoid engaging in certain types of political activity, including activity on social media, that is prohibited by the Hatch Act, 5 U.S.C. §§ 7321-7326. The U.S. Office of Special Counsel (OSC) has posted guidance regarding when Federal employees' use of social media could violate the Hatch Act online at: https://osc.gov/Pages/Hatch-Act-Social-Media-and-Email-Guidance.aspx.

  For further guidance regarding the Hatch Act's prohibitions or particular questions about how the Hatch Act might apply to an OPM planned use of social media, please contact the OPM Office of the General Counsel (OGC).

- **Grassroots Lobbying:** OPM annual appropriations authorizations prohibit the use of appropriated funds for indirect or grassroots lobbying in support of or in opposition to pending legislation. OPM agency users authorized to use social media in their official capacity must not post content on behalf of OPM that includes requests to contact a member of Congress, a jurisdiction, or an official of any Government entity (Federal, state, or local) to favor or oppose any legislation, law, or appropriation because such grassroots lobbying activities are prohibited by Federal law.

- **Discrimination and Harassment:** All employees have a responsibility to maintain an appropriate level of professional conduct in the workplace, and to treat fellow employees with respect and fairness. Pursuant to the OPM Anti-Harassment Policy, OPM prohibits harassing conduct (sexual or non-sexual) in any OPM workplace or in any work-related situation at any other location during or outside normal duty hours. OPM also prohibits retaliation against an employee who alleges harassment, as already defined above, or who assists in any inquiry related to allegations of harassment. Additionally, pursuant to the OPM Anti-Discrimination Policy, OPM prohibits harassment or discrimination directed against fellow employees based on race, color, religion, national origin, sex (including pregnancy and gender identity), national origin, age, disability, or genetic information. OPM also prohibits discrimination based on sexual orientation, marital status, political affiliation, parental status, military services or any other non-merit factor. See 5 U.S.C. §§ 2301- 2302 (prohibited personnel practices).

- **Children:** Agency Web sites or social media accounts must not collect any personal information from children (under the age of 13) in violation of the Children's Online Privacy Protection Act. 15 U.S.C. §§ 6501-6505.

## 7.0 OFFICIAL USE OF SOCIAL MEDIA

When authorized by your supervisor, OPM agency users are permitted to access and contribute content on social media sites in their official capacity. However, agency users must obtain supervisory and program office approval as well as OC approval prior to creating an official OPM social media account and should administer the account in a manner consistent with OC guidelines for content, standards, and best practices. [4] Further, all official OPM web and social media points of contact must be part of the OPM Web Council. All approved social media accounts may engage in recurring exchanges with the public in a manner consistent with this policy, OC guidance, applicable law, and other related guidance.

Agency users will know that they are authorized to communicate in their official capacity when their supervisor assigns this activity as part of the user's official duties. The supervisor should clearly explain the assignment and what social media tool or tools the user is authorized to use and the purpose of the social media tool(s). Program office leadership and OC should also be notified who is managing their social media account(s). Official use is different from an agency user's "personal" use. The important point is that when a user is communicating in an official capacity he or she is communicating on behalf of OPM, just as if he or she was standing at a podium at a conference, communicating the agency's views to everyone.

### 7.1 – TYPES OF OFFICIAL OPM SOCIAL MEDIA ACCOUNTS

All of OPM benefits from a strong enterprise brand, embodied by OPM.gov. Social media helps to extend this brand online and further into the public sphere, using a two-tiered approach:

1. **OPM.GOV-Branded Accounts.** A strong, well-developed enterprise social media brand is the primary tier of this agency's social media strategy. This tier includes any official OPM presence on a social media platform that is managed by OC staff. OPM Program Offices are encouraged to contribute content and ideas to these accounts by contacting OC staff with suggestions.

2. **OPM Program-Specific Social Media Accounts.** On a limited, case-by-case basis, OC and CIO will approve written requests from OPM program and staff offices for their own official OPM social media accounts. Requests are typically approved when (1) there is a clear benefit from external office-specific stakeholder outreach that is not already being met by OPM.gov-branded social media efforts and accounts; and (2) the office making the request has developed an effective strategy to acquire and maintain a stakeholder audience on social media. These OPM program-specific social media accounts are subject to the

[4] This policy is consistent with and does not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to: (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this policy and are controlling. 5 U.S.C. § 2302(b)(13).

same restrictions and limitations as the OPM.gov-branded accounts.

Program offices must obtain OC approval for proposed content prior to posting such content to program-specific social media accounts. Moreover, the program office staff must give OC administrator rights to any and all OPM program-specific social media accounts. OC may deactivate a social media account if the program office managing the account does not comply with the terms of this policy. Program offices interested in establishing a new program-specific social media account should refer to the *Procedures on Establishing and Managing Program-Specific Social Media Accounts contained in Appendix A.*

### 7.2 – TERMS OF SERVICE (TOS) AGREEMENTS

A Federally compatible Terms of Service (TOS) [5] agreement is required for official government use of social media tools. These are special agreements, usually negotiated by the General Services Administration (GSA), with vendors who offer free social media tools. On a case-by-case basis, a service without a GSA-negotiated TOS may be approved for OPM use provided that OGC negotiates a Federally-compatible TOS on behalf of OPM. Federally compatible TOS agreements modify or remove problematic clauses in standard TOS agreements, and allow Federal agencies to use these tools without committing a violation of law. While these – Federally-compatible TOS agreements resolve the major legal issues of the sign-up process, OPM must still comply with laws and regulations on security, privacy, accessibility, records retention, ethical use, and other specific OPM policies and requirements when using the tools. OPM staff, managers, program or field offices are not authorized to negotiate or sign Terms of Service agreements with social media sites on behalf of OPM. OPM may not use social media platforms whose TOS are incompatible with Federal law, regulation, and practice.

Once a third-party site has been approved for use by OC, CIO and OGC, OC will sign these federal-compatible TOS agreements on behalf of OPM.

### 7.3 – OFFICIAL AGENCY SOURCES OF INFORMATION

All content posted to third-party sites should also be available through an agency's official website or by other means. In other words, the public should also be able to obtain comparable information and services through an agency's official website or other official means. (This provision should also help to prevent inadvertent disclosure of non-public information). For example, members of the public should be able to learn about the agency's activities and to communicate with the agency without having to join a third-party social media website. All official OPM third-party social media sites should also provide a link back to the OPM official website. In addition, if an agency uses a third-party service to solicit feedback, the agency should provide an alternative government email address where users can also send feedback.

### 7.4 – RECORDS MANAGEMENT POLICY

Social media allows individuals to collaborate on, create, organize, edit, comment on, combine, and share content, likely resulting in the creation of Federal records. The laws, regulations and policies that govern proper records management apply when using social media, and controls must be established in order to appropriately capture Federal records. The Federal Records Act (44 U.S.C. § 3301) defines records as: includes all recorded

[5] Also known as a "Terms of Use" agreement.

information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. Social media content that meets this definition must be managed according to the applicable laws and regulations.

The maintenance of official OPM social media account records is the responsibility of the program office originating the content. Refer to 36 CFR, Chapter XII, Subchapter B, for guidance on how agencies should apply the statutory definition of Federal records. The following non-exhaustive list of questions will help OPM program offices determine record status of social media content:

- Does it contain evidence of an agency's policies, business, or mission?
- Is the information an exchange with members of the public that follows the discussion of the original post, and therefore, only available on the social media site?
- Does the agency use the tool to convey official agency information?
- Is there a business need for the information?

If the answers to all of the above questions are yes, then the content is likely to be a Federal record. Also, social media content may be a Federal record when the use of social media provides added functionality, such as enhanced searchability, opportunities for public comment, or other collaboration.

Records in social media sites that meet the definition of any agency record must be copied or otherwise captured and maintained with related records throughout the records lifecycle in accordance with approved records disposition schedules. A complete Federal record must have content, context, and structure along with associated metadata (e.g., author, date of creation). The complete record must be maintained to ensure reliability and authenticity. Please note that, because of their uniqueness, comments posted on and messages received through OPM pages are generally considered Federal records and thus may also be subject to public release under FOIA or subject to preservation holds, subpoenas, and document production in the discovery phase of litigation. For assistance with social media records management issues contact OPM's Agency Records Officer. For assistance with preservation, subpoena, and/or discovery obligations, contact OGC.

OC reserves the right to maintain content posted on third-party social media sites until OPM deems that they are superseded, obsolete, or no longer needed for business at which point they will be properly captured and handled per OPM's records management policy.

### 7.5 – Private or Direct Messages From Official OPM Social Media Accounts

The 2014 amendments to the Federal Records Act made several substantive changes that impact electronic records management. The changes include adding requirements for managing electronic messages created or received in non-official and personal electronic messaging accounts. The term "electronic messages" has been defined by statute to mean "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals." 44 U.S.C. § 2911(c)(1). Pursuant to 44 U.S.C. § 2911(a), an employee of an executive agency, such as OPM, may not create or send a record using a non-official or personal account unless they:

- Copy an official electronic messaging account in the original creation or transmission of the record; OR

- Forward a complete copy of the record to an official electronic messaging account not later than 20 days after the original creation or transmission of the record.

Violation of 44 U.S.C. § 2911 could result in the agency pursuing disciplinary action appropriate to the circumstances.

Due to the potential preservation issues, it is OPM policy that OPM social media accounts may not send direct or private messages on social media platforms. If individuals' public comments on or to an OPM social media account warrant a non-public response, the OPM social media account administrator(s) should publically comment on the post and ask the individuals to email their specific questions to an official OPM email account.

### 7.6 – Account Management and Content Considerations for Official Accounts

***Implied Endorsements***

Agency users assigned to administering an official OPM social media account must consider the value in having the OPM account "like" or "follow" another social media account and what that may convey to the social media users who follow the official OPM account. The determination of whether the posting of a hyperlink constitutes an endorsement hinges largely on the unique facts of a situation. See GAO Decision B-326944 (Dec. 14, 2015). In some cases, following another organization may convey endorsement of the entire entity, while retweeting or reposting content from another entity may imply endorsement only of the content that is being reposted. Official OPM social media accounts may not post content that suggests that OPM or any part of the executive branch endorses an organization (including a nonprofit organization), product, service or person. Therefore, generally speaking, OPM programs should avoid linking to external links without prior OC and OGC approval. Links to non-Federal, non-military, or non-state or local government websites are considered "external" links. While there are some known quasi-governmental, educational (.edu), not-for-profit and other types of acceptable sources for linking that are not purely Federal Government, each program office is responsible for analyzing the merits and making a proposal to OC and OGC as to whether or not such a link(s) is/are acceptable for use on official OPM social media accounts.

***Hatch Act Considerations***

According to OSC, use of a Federal agency's official social media accounts, similar to its official website, should be limited to official business matters and remain politically neutral. Thus, an agency's social media account should not "friend," "like," "follow," "tweet," or "retweet" about a partisan group or candidate in a partisan race or link to the social media accounts of such entities. Any information or links to information about a Federal agency official's attendance or speech at a political event for a candidate in a partisan race should not be posted on the agency's Facebook or Twitter account. However, a Federal agency may continue to "friend," "like," or "follow" the official government Facebook or Twitter account of the President or Member of Congress, even after the President or Member begins his or her reelection campaign.

***Respecting Third-Parties' Intellectual Property Rights***

Agency users assigned to administering an official OPM social media account must respect third-parties intellectual property rights. Agency users must comply with the Copyright Law of the United States of America and related laws contained in Title 17 of the United States Code and other Federal policies and directives when posting images, text, video, and audio files protected by copyright on official OPM blogs or third-party social media accounts. For questions regarding copyright matters, please contact the Office of the General Counsel.

***All OPM-Authored Social Media Posts Must Identify OPM as the Source***

In December 2015, the U.S. Government Accountability Office (GAO) issued a decision 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). Pursuant to that decision, employees of OPM are prohibited from asking social media users to post a government-authored message to their social media networks, unless the message expressly states the name of the Federal agency that was the source of the message.

**7.7 – REQUIRED DISCLAIMER FOR ALL OFFICIAL THIRD-PARTY OPM SOCIAL MEDIA ACCOUNTS**

The following disclaimer language must be posted or linked to on all third-party social media tools/sites used by OPM:

> *In order to better serve the public, OPM maintains accounts on third-party websites, such as social media sites, as tools for communicating with the public. Submitting personal information (address, telephone number, email address, etc.) is discouraged and is not required to interact with OPM's accounts on third-party websites, or to access information on any OPM social media site.*
>
> *To protect your privacy and the privacy of others, please do not include your 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. If you have specific questions regarding an OPM activity or program that involves details you do not wish to share publicly, please contact the program point of contact listed at https://www.opm.gov/about-us/contact-us/.*
>
> *In addition, your activity on third-party websites is governed by the security and privacy policies of the third-party sites. Please note: certain information associated with your account may be made available to us based on the privacy policies of the third-party website and your privacy settings within that website. Each third-party website may have unique features or practices. You may wish to review the privacy policies of the sites before using them in order to understand how the information you make available on those sites will be used. You should also adjust privacy settings on your account on any third-party website to match your preferences.*
>
> *OPM uses non-government third-party tools and websites, including social media channels, to provide the public with information in more places and more ways than were traditionally available. Many of these platforms offer the ability for individuals to offer their comments. We encourage members of the public to offer these comments as they relate to the topics being discussed. The views expressed in the comments reflect only those of the comment's author, and do not necessarily reflect the official views of the Office of Personnel Management, its component agencies, or the Federal Government.*
>
> *We reserve the discretion to hide, delete or not allow comments that contain:*
>
> - *Vulgar or abusive language;*
> - *Personal or obscene attacks of any kind;*
> - *Offensive terms targeting individuals or groups;*
> - *Threats or defamatory statements;*
> - *Links to any site;*
> - *Suggestions or encouragement of illegal activity;*

- *Multiple successive off-topic posts by a single user or repetitive posts copied and pasted by multiple users, or spam;*
- *Unsolicited proposals or other business ideas or inquiries;*
- *Promotion or endorsement of commercial services, products, or entities; or*
- *Personally identifiable information that has been inappropriately posted*

*Visitor-generated comments (including username and any identifying information provided) on any and all OPM social media channels become publicly available, both at the time of posting and later, pursuant to FOIA/Privacy Act requests, as applicable.*

*Under the Children's Online Privacy Protection Act of 1998, persons under the age of 13 years old are not allowed to submit questions or comments.*

*If you are a member of the media, please contact the OPM Office of Communications by calling 202-606-2402 or emailing Media@opm.gov.*

*Visit www.opm.gov for information on how to send official correspondence to OPM. Any official policy, regulation, or other information will be published on www.opm.gov, whether or not it is simultaneously posted on third-party social media sites. Only the version published on an official OPM website may be considered official. If OPM "likes" or "follows" of a third-party's social media account should not be construed as an OPM endorsement of that third party. To view our entire Social Media Policy please see www.opm.gov.*

**7.8 – REQUIRED DISCLAIMER FOR ALL OPM-HOSTED SOCIAL MEDIA TOOLS**

The following disclaimer language must be posted or linked to on all OPM-hosted tools (e.g., blogs posted to OPM.gov and THEO):

*In order to better serve its stakeholders, OPM utilizes user engagement tools on OPM-hosted sites, such as blogs on OPM.gov, as tools for communicating with applicable stakeholders.*

*To protect your privacy and the privacy of others, please do not include your social security number, case numbers, or any other sensitive personally identifiable information (PII) in your comments or responses on OPM-hosted communications tools. In addition, please do not include others' social security numbers, case numbers, or any other sensitive personally identifiable information (PII). Our OPM-hosted communications outlets, such as blogs on OPM.gov, should not be considered secure; sensitive or personally identifiable information (PII) should not be shared on these platforms or tools. If you have specific questions regarding an OPM activity or program that involves details you do not wish to share publicly, please contact the program point of contact listed at https://www.opm.gov/about-us/contact-us/.*

*OPM uses OPM-hosted tools and websites, including social media channels, to provide our stakeholders with information in more places and more ways than were traditionally available. Many of these platforms offer the ability for individuals to offer their comments. We encourage our stakeholders to offer these comments as they relate to the topics being discussed. The views expressed in the*

*comments only reflect those of the comment's author, and do not necessarily reflect the official views of the Office of Personnel Management, its component agencies, or the Federal Government.*

*We reserve the discretion to hide, delete or not allow comments that contain:*

- *Vulgar or abusive language;*
- *Personal or obscene attacks of any kind;*
- *Offensive terms targeting individuals or groups;*
- *Threats or defamatory statements;*
- *Links to any site;*
- *Suggestions or encouragement of illegal activity;*
- *Multiple successive off-topic posts by a single user or repetitive posts copied and pasted by multiple users, or spam;*
- *Unsolicited proposals or other business ideas or inquiries;*
- *Promotion or endorsement of commercial services, products, or entities; or*
- *Personally identifiable information that has been inappropriately posted*

*Individual employees, contractors, and interns are not authorized to speak to the media. Members of the media may contact the OPM Office of Communications by calling 202-606-2402 or emailing Media@opm.gov.*

*Visitor generated comments made on any and all OPM social media channels become publicly available.*

*Under the Children's Online Privacy Protection Act of 1998, persons under the age of 13 years old are not allowed to submit questions or comments.*

*Visit www.opm.gov for information on how to send official correspondence to OPM. To view our entire Social Media Policy please visit www.opm.gov.*

**7.9 – PAPERWORK REDUCTION ACT REQUIREMENTS**

Some OPM uses of social media may be subject to the Paperwork Reduction Act (PRA), which governs the solicitation and collection of information from the public by or for the Federal Government, whether that collection is voluntary or mandatory, and regardless of the format. The Office and Management and Budget (OMB), which administers the PRA, approves covered information collections, has issued a memorandum entitled "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act," (April 7, 2010), to help clarify which government uses of social media require OMB approval of an Information Collection Request (ICR) and which do not.

Of particular note, the OMB document distinguishes uses of social media that are akin to general solicitations of comment that might be posed in a Federal Register notice or public meeting (and which do not require approval under the PRA) from use of social media to conduct surveys (which does require approval).

Before using social media to pose questions or invite comments on particular topics, please consult the OMB memorandum and CIO to determine whether the proposed activity requires preparation and approval of an ICR package. Adhere to ICR processes and procedures when applicable.

### 7.10 – THIRD-PARTY INFRINGEMENT OF OPM INTELLECTUAL PROPERTY

OGC is responsible for pursuing steps necessary to protect OPM intellectual property from infringement and/or unauthorized use. Issues involving third parties' improper use of OPM intellectual property on social media accounts should be referred to OC to verify that the alleged improper use is by an entity that is not affiliated with OPM. OC will then, at their discretion, refer the matter to OGC for appropriate action. Should OGC believe that the agency's intellectual property rights have been infringed by the third-party social media account, OGC will prepare a response for the social media company for OC's signature and submission. Only the OC Director (or designee) may complete a social media company's online dispute form on behalf of OPM.

### 7.11 – ACCESSIBILITY

Content posted or produced through the use of new technologies must be accessible to people with disabilities and in compliance with Section 508 of the Rehabilitation Act of 1973. (http://www.section508.gov/section-508-of-the-rehabilitation-act). A relevant link directing users to the accessible content should be made reasonably available on any Web site on which OPM content is not fully accessible. For more information on creating accessible video and social media, visit: https://www.section508.gov/content/build/create-accessible-video-social.

### 7.12 – SOLICITING OFFICIAL PUBLIC COMMENT

OPM will not solicit consensus advice from the public using social media technologies. The Federal Advisory Committee Act (FACA), 5 U.S.C. app., prohibits agencies from receiving consensus advice from *de facto* committees or groups that arise outside of the structure and public scrutiny of a formally established advisory committee. Soliciting consensus advice is seeking input from the public with the intent to obtain advice, opinions or recommendations from the group acting in a collective mode. This is different from general feedback or surveys, polls, etc. that seek to obtain general information or the individual viewpoints of members of the public. For more information on the applicability of the Federal Advisory Committee Act (FACA), see: http://www.gsa.gov/portal/content/100794.

If the social media site allows the public to respond to official postings, OPM must also provide visitors with the ability to communicate with the agency so that members of the public do not have to register with or provide personal information to third-party Web sites that may require registration or the provision of personal information. The OPM site must provide an alternative way, e.g., e-mail address, for members to communicate directly with the agency without providing personal information to a third-party Web site.

### 7.13 – BRANDING

All official OPM social media sites and content must clearly identify ownership or sponsorship through the use of OPM or OC-approved program level branding.

### 7.14 – ERRORS IN OFFICIAL POSTS

In the event there is an error or inaccuracy in an official OPM post, employees, contractors, and non-paid interns should email socialmedia@OPM.gov, to provide the corrected information. All observations will be confirmed and, if an error was made, a correction will be made through that service.

## 8.0 NON-OFFICIAL/PERSONAL USE OF SOCIAL MEDIA

Non-official/Personal use of social media is the day-to-day use of social media sites by agency users that is not related to official duties. Pursuant to the Standards of Ethical Conduct for Executive Branch Employees agency users must be careful in their personal participation in social media sites; they must not engage as if presenting the official position of OPM. According to guidance issued by the Office of Government Ethics (OGE), an employee is not required, ordinarily, to post a disclaimer disavowing government sanction or endorsement on the employee's personal social media account. Where confusion or doubt is likely to arise regarding the personal nature of social media activities, however, an employee is encouraged to include a disclaimer clarifying that the social media communications reflect only the employee's personal views and do not necessarily represent the views of the employee's agency or the United States. A clear and conspicuous disclaimer will usually be sufficient to dispel any confusion that arises. See OGE Legal Advisory LA-14-08. Further, agency users must comply with the OPM Policy on Personal Use of Government Office Equipment and other applicable policies and procedures. Agency users must also be aware that misconduct committed on a social media site may result in appropriate discipline consistent with federal law and agency policy and practice.

### 8.1 – Standards of Ethical Conduct for Executive Branch Employees

The Standards of Ethical Conduct for Executive Branch Employees do not prohibit executive branch employees from establishing and maintaining personal social media accounts. As in any other context, however, employees' social media activities, both inside OPM on the intranet and publically on the internet, must comply with the Standards of Ethical Conduct and other applicable laws, including agency supplemental regulations and agency-specific policies. Failure to comply may result in referral to appropriate law enforcement or appropriate discipline consistent with federal law and agency policy and practice.

The Office of Government Ethics (OGE) has issued OGE Legal Advisory LA-15-03 on the Standards of Ethical Conduct as applied to Personal Social Media Use. Agency users should ensure their non-official/personal use of social media complies with applicable law and OGE guidance.

### 8.2 – Hatch Act Restrictions

Employees must avoid certain types of political activities that are prohibited by the Hatch Act, 5 U.S.C. §§ 7321-7326, including engaging in political activity while on duty and soliciting political contributions. Issues related to employee use of social media can arise under the Hatch Act, particularly as it relates to endorsement of political fundraising activities. The U.S. Office of Special Counsel (OSC) has posted guidance regarding when federal employees' use of social media could violate the Hatch Act online at: https://osc.gov/Pages/Hatch-Act-Social-Media-and-Email-Guidance.aspx. Agency users should ensure their non-official/personal use of social media complies with applicable law and OSC guidance.

This policy creates no new standards, legal obligations, or restrictions on employee conduct, and nothing in this policy should be construed to enlarge or diminish any preexisting rights of employees or otherwise affect terms of employment with OPM.

# APPENDIX A

## OPM Procedures on Establishing and Managing Program-Specific Social Media Accounts

As with any externally facing communications activity, proper management of social media accounts requires an ongoing commitment of time and resources; before creating a new account, a plan describing how the account will be maintained, updated, and monitored on a timely basis should be formed. Offices are urged to think carefully about whether their social media goals could be adequately met by working with OC to promote their content and programs on the pre-existing OPM social media accounts, whose posts regularly reach a substantial audience of users.

### 1. Establishing New Social Media Accounts or Activities

OPM program offices must obtain review and approval from the Office of Communications (OC) and Chief Information Officer (CIO) before implementing any social media site on behalf of OPM or an OPM program. OPM must comply with all applicable Federal laws, rules, and regulations. Any social media accounts or presences representing to be on behalf of OPM or an OPM-program that have not been approved by the OPM Digital Director in OC may be terminated. Please consult with the applicable OPM Social Media Point-of-Contact (SMPOC) before completing a Social Media Request, Attachment 1. OPM Program Offices must complete a separate Social Media request for each requested account. For example, if an OPM program office is requesting both a Facebook and Twitter account, two separate requests must be completed. Once approved, the SMPOC should forward the request to the OPM Digital Director in OC for further review and approval.

All administrators of an OPM program office's social media account must complete mandatory social media training, administered by OC, before beginning to use the OPM-program social media account. Additionally, all administrators should become a part of the OPM Web Council that meets on a regular basis to discuss web and social media issues throughout OPM and conduct regular trainings and best practices seminars. OPM program offices must give administrative rights to OC staff for every program-specific social media account. Contact the OPM Digital Director for more information.

When the new social media account is created, the account must post or link to the comment policy detailed in section 7.6 of the OPM Social Media Policy.

### 2. Registering New Social Media Accounts on the U.S. Digital Registry

The U.S. Digital Registry serves as the authoritative resource for agencies, citizens and developers to confirm the official status of social media and public-facing collaboration accounts, mobile apps and mobile websites. Data fields in the registry include the agency, platform, account, language, points of contact and collaborative tags. The U.S. Digital Registry includes only accounts that represent official U.S. government agencies, organizations, or programs. Accounts managed by Federal agencies and heads of agencies may be registered. Personal, employee, or other types of accounts, however, should not be registered.

Administrators of OPM programs' social media accounts must work with the Office of Communications to register their accounts on the U.S. Digital Registry.

### 3. Transferring Ownership, Admin Rights, and/or Responsibility for a Social Media Account

When an OPM program office needs to make a change to the administrators responsible for the program-specific social media account, the following actions must occur:

- Notify OC before the change needs to occur. Include whether the change in ownership is simply to a different administrator or to an entirely different organization within OPM.
- The new administrator should work with OC to receive any required social media training before he or she is added to the OPM all social media POC meetings and discussions.
- Once all training has been completed, the administrative rights for the OPM program-specific account should be given to the new social media contact.
- Administrator rights for the departing administrator should be revoked immediately when such individual separates from service with OPM or is transferred to a different role.

### 4. Deactivating a Social Media Account

If the decision is made that a social media site should be deactivated, for instance, because it is no longer of use, is no longer accomplishing its goals, or otherwise does not comply with agency policy, the site may be deactivated once the following actions have been completed:

- Notify OC of the program's desire to deactivate the site and specify the reason in writing.
- Confirm all records management requirements to preserve content related to the account have been satisfied.
- Set a time-line for deactivating the site.
    - When will the process begin?
    - When should the site be entirely taken off-line?
        - Be sure to consider that each social media site has its own timeline for taking sites offline. It may be several weeks before the page is no longer viewable. Be sure to integrate this into the proposed timeline.
- Develop a "sign-off" message to post on the site. Depending on the social media site, this will vary in length and tone. However, the following components should always be included:
    - Convey that the site will be going away and when this will occur.
    - Inform your audience/community of other options for interacting with OPM at *(insert relevant social media site(s)* such as @USOPM on Twitter, Feds Hire Vets on Facebook, etc.) This will also vary from site to site but should always, at least, include the OPM.GOV-Branded account.
- Post "sign-off" message during final days/weeks. Post a final goodbye on the last day.
- Do not delete the account entirely lest another entity pick up the account and proceed as if they are acting on OPM's behalf, in their stead, etc.
- Confirm to OC that the site is entirely deactivated.
- Be mindful that some social media providers may automatically deactivate accounts that have not been used over a period of time. Routinely monitor the email account registered with the social media site and, in particular, pay attention for notifications regarding deactivation of the account.


**U.S. Office of Personnel Management**

**Office of Communications**
**1900 E Street, NW, Washington, DC 20415**

**OPM**.GOV

OC-SMP-02931-07-17