



Approved On: 09 FEB 2018

DOJ Instruction

SOCIAL MEDIA CONTENT MANAGEMENT REQUIREMENTS AND PROCEDURES

PURPOSE: Provides guidance in accordance with DOJ Social Media Policy Statement, 0300.02, on components' responsibilities for content management for social media.

SCOPE: All DOJ components

ORIGINATOR: Office of Public Affairs

CATEGORY: (I) Administrative, (II) Government and Public Relations

AUTHORITY: 44 U.S.C. § 3101; 28 C.F.R. § 0.75(j); Presidential Memorandum of January 21, 2009 (Transparency and Open Government); Office of Management and Budget Memorandum of June 25, 2010, Guidance for Agency Use of Third-party Websites and Applications; DOJ Policy Statement 0300.02, Use of Social Media to Communicate with the Public, dated January 19, 2017; DOJ Order 0601, Privacy and Civil Liberties, dated February 6, 2014

CANCELLATION: None

DISTRIBUTION: Electronically distributed to those listed in the "Scope" section and posted to the DOJ directives electronic repository (SharePoint) at: <https://portal.doj.gov/sites/dm/dm/Pages/Home.aspx>

APPROVED BY: *Sarah Isgur Flores*
Director
Office of Public Affairs



ACTION LOG

All DOJ directives are reviewed, at minimum, every 5 years and revisions are made as necessary. The action log records dates of approval, recertification, and cancellation, as well as major and minor revisions to this directive. A brief summary of all revisions will be noted. In the event this directive is cancelled, superseded, or supersedes another directive, that will also be noted in the action log.

Action	Authorized by	Date	Summary
Initial Document	Sarah Isgur Flores, Director, PAO	2/9/2018	Provides the requirements and procedures for components seeking approval from the Social Media Working Group to use social media tools for public communication regarding DOJ mission and functions; provides guidance on components' responsibilities for content and account management for social media tools

TABLE OF CONTENTS

DEFINITIONS	4
ACRONYMS	6
I. Social Media Management	7
II. Content Management	7
A. General Requirements	7
B. Moderating Comments from the Public	8
C. Directly Interacting with the Public	9
D. Linking, Following, and Reposting	9
III. Ethics	10
A. Endorsements	10
B. Private Gain	11
C. Non-public Information	11
D. Political Activity	11
IV. Records Management	11
A. Requirements	11
B. Approval	11
C. Records Retention Schedules	12
D. Deletion or Disposition of Records	12
E. Capstone Officers' Electronic Messages	12
V. Privacy	12
A. Privacy Laws	12
B. Approval	12
C. Initial Privacy Assessment	12
D. Privacy Notice	14
F. Personally Identifiable Information	14
V. Construction	15

DEFINITIONS

Term	Definition
Capstone	An approach developed by the National Archives and Records Administration that categorizes and schedules records based on the work or position of an individual. This approach requires the capture of all business records from individuals at or near the top levels of an agency (or an organizational subcomponent) to be preserved as permanent.
Capstone Official	Any person who serves in a formally designated Capstone position in accordance with Department of Justice (DOJ) Policy Statement 0801.04, Electronic Mail and Electronic Messaging Records Retention .
Component Account	In this document, when referring to the social media account for a component, it includes any department officials with authority to engage in use of social media in their official capacity. This may include both individual official accounts and institutional accounts.
Initial Privacy Assessment	A tool used to facilitate the identification of potential privacy issues; assess whether additional privacy documentation is required; and ultimately, ensure the Department’s compliance with applicable privacy laws and policies. The Initial Privacy Assessment of social media tools used to communicate with the public is a collaborative effort between the Social Media Coordinators and the Senior Component Official for Privacy.
Make Personally Identifiable Information Available	Any agency action that causes Personally Identifiable Information (PII) to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using a website or application. “Associate” can include activities commonly referred to as “friend-ing,” “following,” “liking,” joining a “group,” becoming a “fan,” and comparable functions.
Personally Identifiable Information	Any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security Number, or biometric records, alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth or mother’s maiden name.

Term	Definition
Privacy Impact Assessment	An analysis, required by the E-Government Act of 2002 , of how information in identifiable form is handled to: ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy; determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system; and examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Social Media Coordinators	The component coordinators of official social media accounts. These positions must be occupied by federal employees.
Social Media	Social media, also known as “Web 2.0” or “Gov 2.0” are web-based tools, websites, applications and media that facilitate the creation and sharing of information through virtual communities and networks.
Social Media Working Group	The group responsible for reviewing and approving component applications that use social media tools for official departmental business. This group (made up of representatives from the Office of Public Affairs, Office of Records Management Policy, Office of Privacy and Civil Liberties, Justice Management Division’s Office of General Counsel, Departmental Ethics Office, and Office of the Chief Information Officer) identifies and resolves any issues generated by component-specific social media use.
Web Content Managers	The points of contact for management of DOJ web sites.

ACRONYMS

Acronym	Meaning
C.F.R.	Code of Federal Regulations
DOJ	Department of Justice
IPA	Initial Privacy Assessment
OMB	Office of Management and Budget
PAO	Office of Public Affairs
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SCOP	Senior Component Official for Privacy
SMWG	Social Media Working Group
U.S.C.	United States Code

I. Social Media Management

A component may use only those social media tools that have been approved by the Social Media Working Group (SMWG) for use by that component. Components are responsible for managing and maintaining posted content and ensuring that the content meets the Department of Justice's (DOJ or the Department) media, privacy, security, ethics, accessibility, and records management requirements.

The following is guidance on the appropriate management of approved social media tools.

II. Content Management

A. General Requirements

1. Compliance with existing requirements: Components are required to comply with applicable laws and guidance, including but not limited to:
 - a. Government ethics rules and regulations, such as 18 U.S.C. §§ 202-209 and 5 C.F.R. part 2635; and Departmental regulations and policies, such as DOJ's Supplemental Standards (5 C.F.R. part 3801) and Employee Responsibilities (28 C.F.R. part 45);
 - b. Rules and regulations on partisan political activities, such as the Hatch Act, 5 U.S.C. §§7321-7326, 5 C.F.R. part 734, and Departmental policies;
 - c. [OMB Memo M-10-23](#), "Guidance for Agency Use of Third-Party Websites and Applications" (June 25, 2010);
 - d. [Release of Information related to Criminal and Civil proceedings, 28 C.F.R. § 50.2](#) (restrictions on extrajudicial speech);
 - e. [United States Attorneys' Manual 1-7.000 on Media Relations](#);
 - f. DOJ Policy Statement 0300.02 and DOJ Instruction 0300.02.01; and
 - g. DOJ component-specific guidelines.
2. Official social media accounts may only be used to post information that may be shared with the public in the course of official business. Discussion of classified information on social media is strictly prohibited.
3. Agency Branding: In general, components should use appropriate branding to distinguish the component's activities from those of nongovernment actors. For example, to the extent practicable, a component should add its seal or emblem to

its profile page on a social media website to indicate that it is an official agency presence.¹

4. Social media coordinators will coordinate with their Senior Component Official for Privacy (SCOP), or an authorized designee, prior to disseminating any Personally Identifiable Information (PII).
5. Section 508: Content posted by DOJ on social media accounts will comply with [Section 508 of the Rehabilitation Act of 1973](#). Under Section 508, agencies must give disabled employees and members of the public access to information that is comparable to access available to others.

When compliance is limited due to technical factors posed by the social media tool, information may be posted to the social media account if a compliant version is also posted on the component's official government website.

6. Components should provide individuals with alternative access to information generated by that component on third-party websites and applications. Members of the public should be able to obtain comparable information and services through an agency's official website or other official means. For example, members of the public should be able to learn about the agency's activities and communicate with the agency without having to join a third-party social media website.²
7. Social media tools must provide a link to the agency's official website.
8. All social media postings must be public.
9. Components, at their discretion, may create more restrictive rules governing use of social media.

B. Moderating Comments from the Public

Many social media tools allow for the submission of user-generated content. The Department has a particular interest in allowing for an open forum on its social media sites. Therefore, moderating comments, including censoring and deleting, is generally prohibited. In exigent and extraordinary situations (threats, unauthorized posting of PII, cyber-attack risk, *etc.*), a component should contact the Office of Public Affairs (PAO) or its component security office for guidance. In addition, a component may consider whether the user comment violates the

¹ See [OMB Memo M-10-23](#).

² See [OMB Memo M-10-23](#).

terms of service of the social media site. If so, the user comment may be reported to the social media site as a violation of its terms of service per the site's reporting requirements. PAO can provide additional guidance, as needed.

C. Directly Interacting with the Public

Interacting directly with an individual, organization, or any other member of the public through social media (specifically, responding to a post or comment by another user) creates privacy, records, ethics, and other concerns that must be considered prior to engaging in such practice. Therefore, interacting directly with any user may occur only after receiving authorization from the SMWG, which may require the component to submit an updated Business Case, IPA and Records Questionnaire.

D. Linking, Following³, and Reposting⁴

1. Components may not provide links to sites that require a paid subscription (sometimes referred to as a "pay wall").
2. Direct messaging is not permitted. When possible, the function should be disabled.
3. When possible, public message threads must be closed (*i.e.* the public's commenting on or replying to government postings should not be permitted).
4. Components may follow official government organizations, including federal, state, tribal, local, intergovernmental and international organizations where the United States is a member (e.g., the United Nations). Components may follow nonprofit organizations if (1) the nonprofit's mission is related to the Department's mission or work; (2) following the organization serves a compelling law enforcement or other Departmental interest or function; and (3) is in compliance with all other policies. Because following may imply endorsement of the entity, components are strongly encouraged to consult with their Ethics Official, SCOP (or an authorized designee), communications/public affairs office, and general counsel's office, before following the social media sites of nonprofit organizations.

³ "Following" is used in this Instruction to encompass terms social media tools may use to describe settings that allow accounts to subscribe to other accounts to receive updates. Examples include "friend-ing," "following," "liking," joining a "group," becoming a "fan," and comparable functions.

⁴ "Reposting" is used in this Instruction to encompass terms social media tools may use to describe the ability for content from one account to be posted, often with attribution, to another account. For example, "Retweeting" on Twitter, or "sharing" on Facebook.

5. Components may link to or repost content generated by government organizations, including federal, state, tribal, intergovernmental and international organizations where the United States is a member if the content is in compliance with all other policies. Because linking to or reposting content may imply endorsement of the entity and/or the content that is being reposted, components are strongly encouraged to consult with their Ethics Official, SCOP (or an authorized designee), communications/public affairs office, and general counsel's office before linking to or reposting content from non-governmental sources. Components should link to or repost content from non-governmental entities only in limited situations and when consistent with the below guidance:
 - a. A component may link to or repost factual (i.e., non-editorial) content from a non-governmental entity when the content: (1) is related to the Department's mission or work; (2) serves a compelling law enforcement or other Departmental interest or function; and (3) is in compliance with all other policies.
 - b. Content that includes commentary and/or opinions must not be reposted from a non-governmental entity unless it is a nonprofit or educational entity with which the Department is engaged in a mission-related activity. Such an entity may include a grantee of the Department or a nonprofit with which the Department is cosponsoring an event.

Examples:

- A component may create an original post with a link to an editorial written by a Justice Department employee (e.g., head of component) and published in a non-governmental publication.
- A component may not repost an editorial from a non-governmental source that approves or disapproves of the component's actions.

III. Ethics

Components will follow the Executive Branch and Departmental standards and requirements, as set forth on the Departmental Ethics Office website, particularly the guidance on Misuse of Position 5 C.F.R. §§ 2635.702-703: <https://www.justice.gov/jmd/misuse-position-and-government-resources>.

A. Endorsements

Components may not use social media to endorse any product, service, or enterprise or give the appearance of governmental sanction, except in furtherance of statutory and official authority to promote products, services or enterprises. 5 C.F.R. § 2635.702(c).

B. Public Office for Private Gain

Components may not use social media in a manner intended to induce, coerce or otherwise further the individual private gain of government officials or the private gain of persons or organizations with which the officials are affiliated in a nongovernmental capacity. 5 C.F.R. § 2635.702.

C. Non-public Information

Components may not use social media to publish non-public information or information clearly unauthorized for disclosure. If a component is unsure whether information is public, the component must consult with their SCOP, or an authorized designee, to determine the status of the information at issue before taking any action to disclose the information to the public.

D. Political Activity

Components may not use social media to engage with or endorse politicians or their staffs or any group or individual that is engaged in political activity, as covered by the Hatch Act. 5 U.S.C. §§7321-7326. The Hatch Act defines political activity as an activity directed toward the success or failure of a political party, a candidate for partisan political office, or a partisan political group. 5 U.S.C. §§ 7323(a), 7324(a).

- Example: A component may not repost a partisan comment seeking the failure of a senatorial candidate.

IV. Records Management

A. Requirements

Components will comply with federal record statutory and regulatory requirements, as well as the Department's policies and guidance, for managing federal records created within, or posted to, social media.

B. Approval

Components will obtain approval from the SMWG for the component approach to managing the records that they create within, or post to, social media. This requires that components provide the SMWG with the [Social Media Records Management Questionnaire](#) for review and analysis, in accordance with DOJ Policy Statement 0300.02.

C. Records Retention Schedules

Components will identify or develop applicable records retention schedules that cover record content created within components or posted to social media.

D. Deletion or Disposition of Records

Components will prevent deletion or disposition of any records created or captured using social media, except in accordance with approved records disposition authority in the form of an applicable General Records Schedule or an approved agency unique records retention schedule.

E. Social Media Posts by Capstone Officials

Components will ensure that any publicly posted content issued by Capstone Officials (or any user delegated authority by the Capstone Official to communicate on his or her behalf) be treated as permanent records in accordance with approved Capstone records retention schedules and Departmental policies on Capstone Officials' records.

V. Privacy

A. Privacy Law & Policy Compliance

Components will comply with all applicable federal privacy laws (including, but not limited to, the [Privacy Act of 1974](#) and the [E-Government Act of 2002](#)), the Department's website privacy policy, and the Department's policies and guidance for managing and protecting PII.

B. Approval

Components will obtain approval from the SMWG for their approach to complying with all privacy requirements when creating a social media account or posting content on a social media tool. This requires that the components provide the SMWG with, at a minimum, an Initial Privacy Assessment (IPA), in accordance with [DOJ Instruction 0300.02.01](#).

C. Privacy Impact Assessment

Components will ensure that all social media tools are covered by a Privacy Impact Assessment (PIA), when required by law or policy, prior to the use of a social media tool.

1. A PIA will be required prior to the use of a social media tool if it is determined to meet the requirements of Section 208 of the E-Government Act of 2002 and Office of Management and Budget (OMB) guidance.
2. An adapted PIA will be required prior to the use of a social media tool that makes PII available to the Department. An adapted PIA will be processed and approved consistent with existing Department policies and guidance for processing and approving a PIA pursuant to Section 208 of the E-Government Act of 2002.
3. An adapted PIA will be tailored to address the specific functions of the website or application, but, an adapted PIA need not be more elaborate than the Department's existing PIAs. The adapted PIA will, at a minimum, describe:
 - a. the specific purpose of the Department or component's use of the social media tool;
 - b. any PII that is likely to become available to the Department or component through public use of the social media tool;
 - c. the Department or component's intended or expected use of PII;
 - d. the entity with which the Department or component will share PII;
 - e. the decision about whether the Department or component will maintain PII and, if it will, for how long;
 - f. the way the Department or component will secure PII that it uses or maintains;
 - g. any other privacy risks that exist and how the Department or component will mitigate those risks; and
 - h. the decision about whether the Department or component's activities will create or modify a "system of records" under the Privacy Act of 1974.
4. A single Department-wide adapted PIA may be used to cover multiple social media tools that are functionally comparable, as long as the Department or component's practices are substantially similar across each social media tool.
5. As part of the IPA process, the Office of Privacy and Civil Liberties will include in its final determination whether the component:
 - a. may claim an existing PIA or adapted PIA for its social media tool;
 - b. will draft a new adapted PIA; or

- c. will draft a new PIA, pursuant to Section 208 of the E-Government Act of 2002.

D. Privacy Notice

Components will, to the extent feasible, post a privacy notice on their social media tool. The privacy notice should include:

1. An explanation that the social media tool is not a Department website or application; that it is controlled or operated by a third party; that the Department's website privacy policy does not apply to the third party; and that individuals may wish to review the privacy policies of those third-party websites or applications before using them to understand how and when those websites collect, use, and share the information individuals make available by using their services;
2. An explanation of how the component will maintain, use, and/or share PII that becomes available through the use of the social media tool, as required by law, OMB guidelines, and DOJ policy;
3. An explanation that, by using the social media tool to communicate with the Department or a component, individuals may be providing non-governmental third parties access to PII;
4. A link directing users to the Department or component's official website;
5. A link directing users to the Department's website privacy policy; and
6. A link to any applicable adapted or other PIAs.

E. Personally Identifiable Information

Social media coordinators will coordinate with their SCOP, or an authorized designee, prior to disseminating any PII, in accordance with the "Content Management" section, above.

Overall, social media coordinators should work with their SCOP, or an authorized designee, if they require further guidance on, and assistance with, complying with all privacy requirements related to the use of social media tools.

VI. Construction

This Instruction is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the Department, its offices, boards, divisions, or entities, its officers, employees, or agents, or any other person.