



Approved On: 09 FEB 2018

## DOJ Instruction

### SOCIAL MEDIA ACCOUNT MANAGEMENT AND APPROVAL

---

---

**PURPOSE:** Provides the requirements and procedures for components seeking approval from the Social Media Working Group to use social media for public communication regarding Department of Justice (DOJ) mission and functions; provides guidance on components' account management responsibilities 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 In the event this directive is cancelled, superseded, or supersedes another directive, that will also be noted in the action log.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
<b>Initial Document</b>	Peter Carr, Acting Director, PAO	2/9/2017	Provides the requirements and procedures for components seeking approval from the SMWG 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
	Sarah Isgur Flores, Director, PAO	2/9/2018	Updates definition for social media, section IIB Security, & adds section III Construction.

## TABLE OF CONTENTS

<b>DEFINITIONS</b> .....	Error! Bookmark not defined.
<b>ACRONYMS</b> .....	<b>5</b>
<b>I. Approval Process for Social Media Tools</b> .....	<b>6</b>
A. Social Media Records Management Questionnaire .....	6
B. Initial Privacy Assessment .....	7
<b>II. Account Management</b> .....	<b>8</b>
A. Contact Information .....	8
B. Passwords .....	8
C. Unique Identifiers.....	8
D. Directories .....	8
E. Disposition of Official Social Media Accounts .....	9
F. Accounts Created Prior to Employment at the Department of Justice.	<b>Error! Bookmark not defined.</b>
G. Unauthorized Accounts .....	<b>Error! Bookmark not defined.</b>
<b>III. Construction</b> .....	<b>10</b>

## DEFINITIONS

Term	Definition
<b>Capstone</b>	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 and permanent preservation of all business records from individuals at or near the top levels of an agency (or an organizational subcomponent).
<b>Capstone Official</b>	Any person who serves in a formally designated Capstone position in accordance with Department of Justice (DOJ or Department) Policy Statement 0801.04, <a href="#">Electronic Mail and Electronic Messaging Records Retention</a> .
<b>Initial Privacy Assessment</b>	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.
<b>Records Manager</b>	An individual responsible for the administration of programs for the efficient and economical handling, protecting, and disposing of records throughout their life cycle.
<b>Social Media Coordinators</b>	The component managers of official social media accounts. These positions must be occupied by federal employees.
<b>Social Media</b>	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.
<b>Social Media Working Group</b>	The group responsible for reviewing and approving component applications to use social media tools for official DOJ business. 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, this group identifies and resolves any issues generated by Department or component-specific social media use.
<b>Web Content Managers</b>	The points of contact for management of DOJ web sites.

## ACRONYMS

<b>Acronym</b>	<b>Meaning</b>
<b>C.F.R.</b>	Code of Federal Regulations
<b>DOJ</b>	Department of Justice
<b>GRS</b>	General Records Schedule
<b>IPA</b>	Initial Privacy Assessment
<b>NARA</b>	National Archives and Records Administration
<b>OPCL</b>	Office of Privacy and Civil Liberties
<b>ORMP</b>	Office of Records Management Policy
<b>PAO</b>	Office of Public Affairs
<b>PII</b>	Personally Identifiable Information
<b>SCOP</b>	Senior Component Official for Privacy
<b>SMWG</b>	Social Media Working Group
<b>U.S.C.</b>	United States Code

## I. **Approval Process for Social Media Tools**

As required by Department of Justice (DOJ or Department) [Policy Statement 0300.02 “Use of Social Media to Communicate with the Public.”](#) components will follow the process outlined below to obtain approval for accounts on public-facing social media tools for official DOJ business.

**STEP 1:** Component Social Media Coordinator submits a [Project Request Form](#) to the [Social Media Working Group](#) (SMWG). The Project Request Form must explain the need and proposed use for the requested social media account.

**STEP 2<sup>1</sup>:** Component submits the following per the procedures below:

### A. **Social Media Records Management Questionnaire**

The Social Media Records Management Questionnaire assists in determining whether content created is a federal record and how to treat those records.

1. The component’s Records Manager, Social Media Coordinator, and component information technology specialists should confer to develop responses to the Social Media Records Management Questionnaire and then submit it to the Justice Management Division, Office of Records Management Policy (ORMP).
2. After ORMP has reviewed the questionnaire responses and has conducted follow-up discussions with the component, ORMP and the component will determine whether the content that is created or captured meets the definition of a federal record, 44 U.S.C §§ 3101, *et seq.*

If the content is not record content, then ORMP will advise the SMWG that the tool does not create or maintain records.

If the content is record content, then ORMP and the component will determine whether the record content falls under a provision of the General Records Schedules (GRS), (36 C.F.R. §1228.40, subpart C) or under an existing National Archives and Records Administration (NARA)-approved or pending DOJ or component schedule.

If the content falls under an existing or pending GRS or DOJ schedule, the component shall follow the required records retention schedule.

---

<sup>1</sup> The Initial Privacy Assessment and the Social Media Records Management Questionnaire in “Step 2” may be submitted in any order, or simultaneously.

If the record content does not fall under an existing or pending GRS or a DOJ schedule, the component will meet the records scheduling requirements below and must maintain the records until a schedule is approved:

- (i) Records Managers for components and the offices, boards, or divisions will submit to ORMP, within 6 months of going live, a draft records retention schedule. ORMP will review and revise the proposed schedule as needed, and submit the final schedule to NARA for approval.
- (ii) Records Managers for bureaus will ensure, within 2 years of going live, that a records retention schedule has been approved by NARA for records created or captured using social media applications.

## **B. Initial Privacy Assessment**

The Initial Privacy Assessment (IPA) is a tool used to facilitate the identification of potential privacy issues; assess whether additional privacy documentation is required; and ensure the Department's compliance with applicable privacy laws and policies. After conferring with its Senior Component Official for Privacy (SCOP), the component must submit an IPA to the Office of Privacy and Civil Liberties (OPCL), in accordance with the requirements of this Instruction and guidance issued by the Chief Privacy and Civil Liberties Officer or OPCL.

1. An IPA for the use of a social media tool should be written and reviewed at the component level through the coordinated effort of the component's privacy officials (*e.g.*, the SCOP, the Privacy Act Officer, or a representative from the component's Office of General Counsel) and the program-specific office responsible for managing the social media tool.
2. Completed IPAs will be submitted to OPCL through the component's OPCL point-of-contact or e-mailed to [privacy@usdoj.gov](mailto:privacy@usdoj.gov). OPCL will review the completed IPAs and issue a final determination about whether additional privacy documentation, such as an Adapted Privacy Impact Assessment,<sup>2</sup> or other privacy-protective measures are required.

**STEP 3:** After review is complete, the [SMWG](#) will contact the component regarding the final determination, and may include requirements for the operation of the social media tool.

---

<sup>2</sup> Per OMB Memorandum M-10-23, [Guidance for Agency Use of Third-party Websites and Applications](#), (June 25, 2010), an adapted PIA is intended to support the management of risk to privacy on a third-party website or application (such as Facebook and YouTube).

## II. Account Management

### A. Contact Information

Only official Department contact information and email addresses may be used in conjunction with the creation and management of official social media accounts. The use of Department organizational email addresses is recommended whenever possible.<sup>3</sup>

### B. Security

Components will follow DOJ security practices outlined in annual Computer Security Awareness training and password requirements available in DOJ Cybersecurity Policy Instruction, [DOJ Cybersecurity Standard, Unclassified Control Matrix](#). Additional information regarding social media is available from the [OCIO Cybersecurity Services Staff, Social Media Best Practices and Vandalism Response Research Publication](#).

### C. Unique Identifiers

The unique identifiers (*e.g.*, Twitter handle, Facebook page name) of official social media accounts must signify affiliation with DOJ.

*Example Twitter Handles: @ComponentName*

*@DOJComponentName or @ComponentNameDOJ*

*@ComponentNameTitle or @TitleOfficial'sName*

Contact the Office of Public Affairs (PAO) with questions or for additional guidance.

### D. Directories

#### 1. U.S. Digital Registry

The Social Media Coordinator must ensure that all of the component's official social media accounts are registered with the [U.S. Digital Registry](#).<sup>4</sup>

---

<sup>3</sup> Organizational email addresses refer to group email accounts that more than one employee can access. An organizational email address might be "component.socialmedia@usdoj.gov" while an individual's Department email address would be "jane.doe@usdoj.gov."

<sup>4</sup> "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, and help prevent exploitation from unofficial sources, phishing scams or malicious entities." DigitalGov <https://usdigitalregistry.digitalgov.gov/> accessed 11/4/16.



2. Department of Justice Directories

The Social Media Coordinator must ensure that all of the component's official social media accounts are listed on the Department's [Social Media Directory](#).

**E. Disposition of Official Social Media Accounts<sup>5</sup>**

Components will use the following procedures when disposing of official social media accounts at the end of an administration or for other reasons:

1. Institutional Accounts

When retiring an institutional account, neither the content nor the account should be deleted. Post a final message that explains that the account is no longer being used and refer people to a site where they can find information on the component. Advise PAO that the account has been retired.

2. Individual Official Accounts (accounts in the name or title of Department officials)

- a. When a government official ends his or her employment with the Department, the government official's authorization to use the social media account on behalf of the Department immediately terminates.
- b. The Department, not the government official, retains ownership of the account and content that the government official created or generated on the social media service and all other rights and benefits associated with the social media account.
- c. Prior to leaving the Department, the government official will ensure that all authorization to access the social media account is transferred to and/or retained by the Department, including, but not limited to, account passwords or other authentication requirements for account access.
- d. Components may, to the extent technically feasible and in accordance with all legal and ethical requirements, assist a departing official's transition away from their departmental social media presence. Assistance may include, but is not limited to, changing any unique identifiers, such as the official's name on the Department's social media account, so that the former government official may use the identifier in his or her personal capacity. Components may also

---

<sup>5</sup> See also attached White House memo "Disposition of Official Social Media Accounts," October 31, 2016.

assist the official by developing and posting a farewell message, provided this notification follows all applicable ethics regulations (*e.g.*, the farewell message does not direct the public to a political campaign). The government official should be aware that the Department is under no obligation to assist, but may do so at its discretion.

- e. When retiring an official individual account, neither the content nor the account should be deleted. Indicators such as the bio should be updated to reflect that the official is no longer with the Department and the account is no longer active.
- f. Contact PAO with questions or for additional guidance.

#### **F. Accounts Created Prior to Employment at the Department of Justice**

Only accounts that have been authorized through the SMWG may be used in an official capacity.

Accounts created prior to an individual's employment at DOJ will be considered personal social media accounts.<sup>6</sup>

#### **G. Unauthorized Accounts**

If a component is using social media tools in an official capacity and has not received approval from the SMWG, the component will immediately contact the SMWG.

### **III. 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.

---

<sup>6</sup> See also, [Guidance on the Personal Use of Social Media by Department Employees](#), March 24, 2014 memo from Deputy Attorney General James M. Cole.