



Approved On:

10 JAN 2018

DOJ Policy Statement

USE OF SOCIAL MEDIA TO COMMUNICATE WITH THE PUBLIC

PURPOSE: Establishes Department of Justice (DOJ or Department) policy and procedures for the approval, use, and management of social media tools that are used to communicate and share information with the public.

SCOPE: All DOJ components

ORIGINATOR: Office of Public Affairs

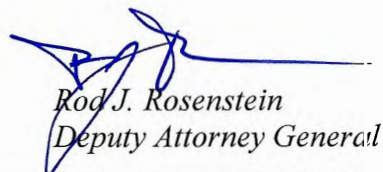
CATEGORY: (I) Administrative, (II) Government and Public Relations

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)

CANCELLATION: Deputy Attorney General Memo “Social Media and Web 2.0,” dated January 29, 2010; Assistant Attorney General for Administration Memo “Web 2.0 Applications,” dated May 8, 2009

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:


Rod J. Rosenstein
Deputy Attorney General

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 In the event this directive is cancelled, superseded, or supersedes another directive, that will also be noted in the action log.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 Approval	Sally Q. Yates Deputy Attorney General	Jan 19, 2017	Establishes Department of Justice policy and procedures for the approval, use, and management of social media tools that enable communication with the public
	Rod J. Rosenstein Deputy Attorney General	Jan 10, 2018	Updates definition for social media, clarifies sections I Policy on scope and III A on the roles and responsibilities of the Social Media Working Group, and adds Section IV Construction.

TABLE OF CONTENTS

ACTION LOG..... 2

DEFINITIONS 4

ACRONYMS..... 5

I. Policy 6

II. Approval for Social Media Tools..... 7

III. Roles and Responsibilities..... 7

 A. Social Media Working Group 7

 B. Head of Component 8

 C. Chief Privacy and Civil Liberties Officer 9

 D. Component Social Media Coordinator..... 9

 E. Component Web Content Managers 10

 F. Senior Component Official for Privacy 10

 G. Component Records Officers or Records Managers..... 10

 H. Component Ethics Officials 10

IV. Construction 11

DEFINITIONS

Term	Definition
Social Media Coordinators	The component coordinators of official social media. 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 to use social media tools for official Department of Justice (DOJ or Department) 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.
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.
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.

ACRONYMS

Acronym	Meaning
CPCLO	Chief Privacy and Civil Liberties Officer
C.F.R.	Code of Federal Regulations
DOJ	Department of Justice
PAO	Office of Public Affairs
OPCL	Office of Privacy and Civil Liberties
SMWG	Social Media Working Group
TOS	Terms of Service
U.S.C.	United States Code

I. Policy

Social media tools provide the technical capability to communicate and disseminate information to the public on behalf of the Department of Justice (DOJ or Department). The Department permits components to use social media tools, conditioned on appropriate approval, to provide information and enhance communication with the public in support of DOJ's mission when such use:

- promotes the mission, goals, and objectives of the Department;
- complies with applicable statutes, regulations, Federal Government-wide guidance, and departmental policies;
- protects individual privacy;
- ensures that federal records are properly maintained;
- complies with applicable ethical standards;
- maintains the security of Department systems and information;
- operates only under Terms of Service (TOS) agreements that have been reviewed and signed by a Department official to ensure compliance with federal laws; and
- is authorized by the Department's Social Media Working Group (SMWG) and managed in accordance with this Policy Statement and corresponding DOJ instructions (including DOJ instructions 0300.02.01 and 0300.02.02) and federal instructions.

This policy applies to all official social media accounts used or managed by Department employees for official business, whether the account is in the name of a Department component, office, official, program, initiative, etc.

This policy does not apply to:

- The use of social media for exclusively internal communications. These tools for internal communication may require other reviews and approvals (including, but not limited to, counsel, component Chief Information Officers, and records officers and managers) and may be subject to other Departmental policy.
- The use of social media as an operational tool in support of: law enforcement or intelligence operations; civil or criminal investigations; or litigation.

- The personal use of social media by Department employees.

Any account that is not created and authorized in accordance with this Policy Statement will be considered an account created in an individual's personal capacity and will be subject to all applicable laws, rules, regulations, and policies regarding the personal use of social media.¹

II. Approval for Social Media Tools

Components must obtain approval from the SMWG before using social media tools for official DOJ business, per processes described in corresponding instructions. The approval process requires components to provide a description and business purpose for the proposed use of the social media tool, document the recordkeeping approach, and complete an Initial Privacy Assessment. During the approval process, the SMWG may request additional information and engage in further discussions with the component.

III. Roles and Responsibilities

A. Social Media Working Group

1. In coordination with the Office of the Deputy Attorney General, develops department policy regarding official use of social media to communicate with the public.
2. Reviews, analyzes and authorizes component requests to use social media to communicate with the public.
3. Provides guidance regarding the use of official social media to components upon request.

The SMWG is composed of representatives from the following offices:

- **Office of Public Affairs** - Chairs the SMWG and is responsible for working with components to align and coordinate the Department's public message and use of social media.
- **Office of the Chief Information Officer** - Distributes social media guidance via DOJNet; coordinates the Quarterly Web Certification, which requires components to certify that their use of social media complies with DOJ and Office of

¹ See also, [Guidance on the Personal Use of Social Media by Department Employees](#), March 24, 2014, memo from Deputy Attorney General James M. Cole.

Management and Budget guidelines; and maintains the Social Media page on justice.gov.

- **Office of Privacy and Civil Liberties** – Defines the high-level privacy requirements for the establishment and use of Department social media tools, in coordination with the Chief Privacy and Civil Liberties Officer (CPCLO).
- **Office of Records Management Policy** – Defines the high-level records management requirements for content posted to social media and reviews and approves component approaches for managing record content created or published using social media tools.
- **Departmental Ethics Office** – Reviews and authorizes the proposed uses of social media consistent with the applicable statutes, standards of conduct for federal employees, and the Department’s standards and requirements for the ethical conduct of departmental business.
- **Justice Management Division’s Office of General Counsel** – Reviews and approves all TOS agreements with social media providers prior to the use of any social media tool and provides advice on other legal issues that arise with respect to the Department’s official use of social media.
- **Additional representatives** – The SMWG may also include other representatives from other components or offices, as the Chair may designate, and the Chair may invite the participation of representatives from other components or offices as she or he deems appropriate.

B. Head of Component

1. Authorizes the proposed use of social media by the component, including the official use of institutional and individual accounts, contingent on approval by the SMWG.
2. Authorizes the application to the SMWG for use of official social media within the component.
3. Ensures that the component is using official social media tools only to the extent that such tools have been authorized for component use by the SMWG.

4. Exercises oversight responsibility for component compliance with all statutory, regulatory, and departmental policies related to the official use of social media for business purposes.
5. Appoints a component Social Media Coordinator to coordinate social media use within the component and with the Office of Public Affairs (PAO) and to ensure collaboration among component business users, records managers or officers, privacy officers, and IT staffs to meet records management, privacy, and technology requirements.

C. Chief Privacy and Civil Liberties Officer

1. Establishes privacy policies and standards for the Department's use of social media.
2. Issues Department-wide advice, guidance, policies, and procedures on issues concerning the interpretation, application, and implementation of DOJ privacy policies and privacy compliance matters related to the use of social media.
3. Oversees the Department's compliance with applicable information privacy laws and policies as they relate to the use of social media.
4. Provides, in coordination with PAO and the SMWG, privacy guidance and awareness training to DOJ personnel regarding the use of social media.

The CPCLO may, as appropriate, delegate the CPCLO's statutory or delegated authority to the Office of Privacy and Civil Liberties (OPCL) and to component officials, subject to the CPCLO's oversight and control.

D. Component Social Media Coordinator

1. Coordinates social media use within the component and with PAO.
2. Ensures compliance with all statutory, regulatory, and departmental requirements (including that such social media tools have been authorized by the SMWG) when the component uses social media tools to communicate information to the public, particularly with respect to security, privacy, and records management.
3. Ensures that all individuals with access to the components' social media accounts have reviewed corresponding DOJ instructions and received related social media guidance prior to assuming responsibility for the account.

4. Serves as the primary point of contact between the component and the SMWG, particularly with regard to requests for new social media tools in accordance with corresponding DOJ instructions.

E. Component Web Content Managers

1. Ensure that the use of social media referenced on their websites complies with departmental requirements.
2. Certify this compliance on the Quarterly Web Certification form.

F. Senior Component Official for Privacy

1. Ensures the proper and timely preparation and completion of required privacy compliance documentation for the operational use of social media by the component.
2. Manages, at the component level, the implementation of privacy policies and requirements for the operational use of social media by the component.
3. Identifies privacy issues, concerns, or risks with the component's use of social media and works with the CPCLC and OPCL to take appropriate steps to address and resolve such privacy issues, concerns, or risks.

G. Component Records Officers or Records Managers

1. Work with component business managers, users, and IT staff to develop reasonable technology, policy, and processes to meet recordkeeping requirements.
2. Determine which records retention schedules apply to content generated within social media tools for the component or, if none are applicable, develop appropriate records retention schedules for the content.

H. Component Ethics Officials

1. Manage, at the component level, identification of ethics issues, concerns, and risks associated with the use of social media.
2. Review and advise on the application of the ethics rules, as set forth in corresponding DOJ instructions. Ethics issues include misuse of position, endorsements and the appearance of government sanction, use of public office for private gain, publication of unauthorized and/or non-public information, public comments on pending investigations and trials, and political activity.

3. Consult with the Departmental Ethics Office, as appropriate, on ethics issues arising from a component's proposed social media postings and application of the Department's social media policy.

IV. Construction

This policy 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.