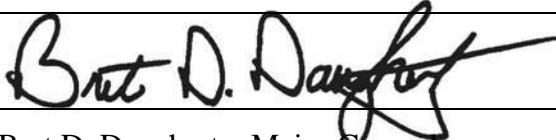




Department Policy No. COMM-902-20

Title	Social Media Policy
Former Number	11-01
References	42.52 RCW Ethics in Public Services Act WAC 292-110-010 Use of State Resources Rule 5 CFR Part 2635, Standards of Ethical Conduct for Employees Governor's Social Media Guide, November 2010 DoDD 5230.9, Clearance of DoD Information for Public Release, 9 April 1996
Information Contact	Communications Director Building 1, 253-512-8222
Effective Date	May 1, 2011
Mandatory Review Date	January 31, 2024
Revised	January 31, 2020
Approved By	 Bret D. Daugherty, Major General The Adjutant General WMD Director

Purpose

The purpose of this policy is to set clear guidelines and direction for the use of social media in the workplace. This policy is not meant to infringe on the employees' right to engage in protected activity and collective bargaining agreement issues related to their wages and working conditions.

Scope

This policy applies to all state employees of the Washington Military Department (WMD).

Definitions

- Social media or social networking:** Interaction with external internet websites or services based on participant contributions to the content. Types of social media may include blogs, micro blogs, social and professional networks, video or photo sharing, and social bookmarking. Examples of social media sites are *YouTube, Facebook, Flickr, Twitter, WordPress, NextDoor, RSS, Medium, Second Life, LinkedIn*, etc.

Policy

A. Permitted Use

Access to social media networks from within the WMD's IT infrastructure is limited to employees who have a clear business purpose to use the forum, and are performing official WMD business,

WMD employees may use social media in the workplace only for approved agency purposes in support of the agency mission, including professional networking, keeping the public informed and educating the public about who we are, what we do and why we are important to them.

WMD employees who engage in social media for agency purposes shall not engage in unlawful or prohibited conduct, and must adhere to applicable policies, including, but not limited to the following:

1. Ethics ([HR-207-03](#)). WMD employees are responsible for knowing and adhering to applicable ethics laws and policies, and for making choices that exemplify adherence to high ethical standards.
2. Sexual Harassment ([HR-226-98](#)). The WMD provides a work environment free from sexual harassment, a form of sex discrimination that violates equal employment laws.
3. Discrimination ([HR-208-01](#)). The WMD prohibits discrimination on the basis of race, color, creed, national origin, sex, marital status, religion, age, sexual preference/orientation, gender identity, or the presence of any sensory, mental, or physical disability in all aspects of service delivery and employment.
4. Use of Internet, Electronic Mail and Computer Systems ([IT-311-18](#); <https://dodcio.defense.gov/DoD-Web-Policy/>) Internet connectivity, electronic mail, and computer systems are provided primarily to send, receive, and store information of an official, work-related nature. Unless specifically provided by this policy, public law, ethics guidance letters and/or government regulation, all other use is prohibited.
5. Teleworking or Alternative Worksites ([HR-225-02](#)). WMD employees must comply with agency standards for social networking when teleworking or working at an alternate worksite.
6. Intellectual Property Protection ([05-00](#)). WMD employees shall comply with the terms and conditions of all licensing agreements and the provisions of the Copyright Act and other applicable laws.
7. Information Technology Security Policy ([IT-302-04](#)). WMD employees shall protect and use agency data and equipment assets in an authorized manner.
8. WMD Records Management Program Policy ([DIR-005-08](#)). WMD employees are responsible for managing the records they create and use in accordance with the Secretary of State's retention schedules.
9. WMD Public Records Disclosure Policy ([DIR-004-08](#)). All records that are used, maintained, accessed or created within WMD are subject to disclosure under the Public Records Act, to include social media.

Users of social media sites should take into consideration the lack of anonymity and exercise sound judgment, including, but not limited to, considering whether usage may impact work performance, office morale or overtime issues.

WMD employees shall not set-up a social media account for agency purposes unless approved in advance under this policy.

Failure to abide by this policy or participation in any activity inconsistent with WMD's values and mission may result in appropriate disciplinary action.

B. Comment Policy

Visitors to social media sites shall be notified that the intended purpose of the site is to serve as a mechanism for communication between WMD divisions and departments and members of the public. More [information on content guidelines here](#). WMD social media site articles and comments containing any of the following forms of content are prohibited:

1. Comments not typically related to the particular social medium article being commented upon;
2. Profane language or content;
3. Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, national origin, physical or mental disability or sexual orientation;
4. Sexual content or links to sexual content;
5. Attempts to sell or purchase products;
6. Illegal conduct or encouragement of illegal activity;
7. Information that may compromise the safety or security of the public or public systems.

C. Personal Use

Employees should understand that words and actions posted to social media may be perceived by others as being representative of our agency, regardless of when, where and how the content was posted. While we acknowledge employee rights to privacy and free speech that may protect online activity conducted on personal social networks, what is published on such personal sites should not be attributed or reference the agency and should not appear to be endorsed by or originated by the agency. Employees that list their work affiliation or reference their employment with the state of Washington and the WMD in any way on a social network should regard all communication on that network as if it were a professional network. If employees identify themselves as a state employee on a social networking site, wherever appropriate, use a disclaimer (e.g. "While I work for a state agency, anything I publish is my personal opinion and not necessarily the opinions or position of my agency or state.")

State ethical obligations must be followed at all times, even when employees engage in social media use in their personal capacities. For example, employees must not disclose confidential information acquired by the employee by reason of the employee's official position. See RCW 42.52.050U.

Employees assume any risk associated with their personal social media use. The WMD may require immediate removal of material and/or take disciplinary action for personal social media use that causes workplace disruption or impairs the WMD's mission.

Employees who use personal social media may not:

1. Use work email or password in conjunction with a personal social media site.
2. Use state-owned resources (computer, network, cell phone, etc.) to access social networking websites unless authorized to do so for official WMD business. Employees must not use any state resources to access social networking sites for political purposes, to conduct private commercial transactions or to engage in private business activities. Please refer to [WAC 292-110-010U](#).
3. Attribute personal statements, opinions or beliefs to our agency or our agency's leadership.
4. Disclose confidential information.
5. Use our agency's logo, the state seal or state logos.
6. Participate on social media websites or other online forums on behalf of an agency unless authorized by the agency head or the agency's communication director or designee.
7. Post material that (i) constitutes harassment, hate speech or libel; (ii) violates fellow employees' privacy; or is (iii) disruptive to the work environment because it impairs workplace discipline or control, impairs or erodes working relationships, creates dissension among co-workers, interferes with job performance or obstructs operations.

D. Privacy

The Internet is an unsecured publicly accessible network. WMD employees should have no expectation of privacy in the use of Internet resources. Owners of Internet sites commonly monitor usage activity and those activities may be disclosed to any number of parties.

The WMD reserves the right to monitor workplace Internet usage at such times and in such circumstances as it deems appropriate.

Social media shall not be used to distribute privileged or confidential material.

E. Responsibilities

All WMD employees who currently have or want to set-up a social media account for agency purposes must complete the Social Networking User Request WMD Form 0002-11 or WMD Form 0002-11-WYA (Just for the Washington Youth Academy) and obtain approval of their division director and the WMD Communications Director.