UNCLASSIFIED

MRN:	21 STATE 33406
Date/DTG:	Apr 07, 2021 / 072233Z APR 21
From:	SECSTATE WASHDC
Action:	ALL DIPLOMATIC AND CONSULAR POSTS COLLECTIVE *IMMEDIATE*
E.O.:	13526
TAGS:	APER, AMGT, KPAO
Reference:	A) 20 STATE 104660 (Annual Reminder: Department Policies on the Use of Social Media for Official Communications) B) 19 STATE 65258 (Political Activities Guidance) C) 20 STATE 71636 (2020 Hatch Act/Political Activities)
Subject:	Department Policies Related to Employees' Use of Personal Social Media and Digital Communication Platforms

1. **Key Points:**

- Employees should be aware of their responsibilities and the potential consequences to official Department business of personal social media activity and communications that occur on digital platforms (such as WhatsApp, texts, emails, and instant messages). Consequences to Department business can include the disruption of Department operations and impairment of working relationships.
- Employees must comply with all applicable Department rules related to activity on personal social media and digital platforms, including Hatch Act limitations and the Department's guidance on political activities.
- Employees who engage in public communications on matters of Departmental concern (as outlined in 3 FAM 4173) through their personal social media accounts must seek advance review. The Bureau of Global Public Affairs conducts this review for employees assigned domestically. Employees assigned abroad must seek review from their Chief of Mission and should abide by post's media policy.
- Employees may not use personal social media accounts for official communications and must not claim to represent the Department, the U.S. government, or U.S. government policies on personal social media accounts (10 FAM 181-182).
- Failure to follow Department policies on personal social media and communications through digital platforms may result in a proposal for disciplinary action, up to and including separation.
- This guidance is not meant to infringe or restrict employees' freedom of expression; it is a reminder that employees should be mindful of how their social media use may interfere with the Department's ability to effectively and efficiently carry out its mission and responsibilities.

Message from the Bureau of Global Talent Management:

2. Technology and how we use it changes rapidly. Social media, in particular, continues to undergo significant advancements. There is no longer any expectation that information posted on social media or exchanged through digital platforms such as WhatsApp, texts, emails, or other messaging forums will remain private, even if shared in a closed group or with just one person. While we cannot always predict the direction in which social media will go, employees must remain ever mindful of how they conduct themselves in virtual environments. We want employees to be fully aware of their responsibilities when it comes to posting, commenting, and sharing information via their personal social media accounts and on digital platforms. While the policies included in this cable are not new, they do serve as a reminder for us all to remain vigilant about our online presence and to remain thoughtful of how we choose to communicate.

Communicating on Personal Social Media Accounts and Digital Platforms

3. This cable provides an overview of existing guidance on employees' personal use of social media. The same guidance applies to any online activity or communication through digital platforms. While employees may believe their activity is safeguarded on internal or closed networks, they must remain mindful that any digital or electronic communication has the potential to become public. Additional guidance can be found in the referenced cables and Paragraph 21.

4. Social media use is considered personal when an employee is:

- Communicating personal views as a private citizen;
- Using a personal social media account; and
- Neither communicating as part of their employment responsibilities nor representing the Department or the U.S. government in any capacity.

5. Personal social media accounts may not be used for official communications on behalf of the Department. Only official social media accounts may be used for official communications, and personal social media accounts utilized for official communications may be retained by the Department (10 FAM 182(c)). The Department has produced additional guidance clarifying how to distinguish official from personal social media accounts (see Ref A, 10 FAM 180, and the Department's Social Media Hub (OpenNet, GO Browser), which includes a Personal and Official Use Social Media Handbook (OpenNet, GO Browser). For example, Department personnel must avoid reposting official content on a personal account in such a routine fashion that the personal account is seen as an alternative source or location for official U.S. government communications or views. Please direct questions to socialmedia@state.gov.

Communicate Responsibly

6. Employees should consider carefully whether their personal social media or other online and digital activity may interfere with the Department's ability to effectively and efficiently carry out its mission and responsibilities, by, for example, disrupting operations, or impeding the

employee from carrying out his or her duties. Remaining professional and courteous can reduce the risk of negative impact to the Department and/or an employee's immediate work unit. Employees should also consider how easily digital activity can be shared and spread through public means even if intended for a private or closed audience.

7. Social media activity or messaging on digital platforms that results in disruption to the efficiency of the service or workplace may impact an employee's assignment, security clearance, performance evaluation, or otherwise have professional repercussions, including disciplinary action. Likewise, when an employee who uses official Department equipment, like their work computer or cell phone, to make or post communication that has a derogatory effect on the mission or workplace, the employee may be subject to disciplinary action. Some examples of potentially disruptive activity or messaging may include:

- Making unfavorable or disparaging comments about one's colleagues or supervisors;
- Referring to a host country or its living conditions in disparaging terms;
- Posting about activities that are illegal or otherwise proscribed in a host country;
- Making jokes about topics that are culturally sensitive in a host country;
- Making comments disparaging to another individual based on race, religion, gender, sexual orientation, disability, or national origin; or
- Posting comments that are critical of or reflect negatively on a mission or a mission's programs.

8. This guidance is not meant to infringe or restrict employees' freedom of expression. Rather, it is a reminder that employees should be mindful of how their social media use may interfere with the Department's ability to carry out its mission and responsibilities. When an employee's social and digital media use negatively affects the mission, the employee can be held accountable for the impact of their actions.

Review of Personal Public Communications on Social Media

9. Employees who wish to comment publicly on matters of Departmental concern on their personal social media accounts or through other public communication means should familiarize themselves thoroughly with the requirements of 3 FAM 4170, including the requirement to seek advance review of any statements that may be of Departmental concern. This section of the FAM should be read and understood as a whole, as many of its provisions interrelate, but a number of them bear special attention in the context of public communications on social media.

10. As a threshold requirement, each employee must make an initial determination as to whether a matter on which he or she wishes to make a statement may be a matter of Departmental concern. 3 FAM 4173 defines "of Departmental concern" as: "Pertaining to current U.S. foreign policy or the Department's mission (including policies, programs, operations or activities of the Department of State or USAID), or which reasonably may be expected to affect the foreign relations of the United States."

11. The process for seeking advance review of personal capacity public communications is described in 3 FAM 4174.3, 4176.3, and 4176.4. The review requirement is intended to serve three purposes: to determine whether the communication would disclose classified or other protected information without authorization; to allow the Department to prepare to handle any potential ramifications for its mission or employees that could result from the proposed public communication; or to identify public communications that are highly likely to result in serious adverse consequences to the mission or efficiency of the Department (3 FAM 4174.2(c)(1)).

12. Unless the final review office indicates otherwise, employees who are authorized to comment personally on a matter of Departmental concern must include a disclaimer indicating that the views expressed are the employee's own and not necessarily those of the U.S. government (3 FAM 4176.1).

13. Employees who, in their personal capacity, wish to comment on matters that are *clearly not* "of Departmental concern" on social media or through other electronic communications, do not need to seek review and need not use the personal capacity disclaimer, as discussed above (3 FAM 4176.1). However, if there is any doubt as to the need to seek review or use a disclaimer, employees should seek guidance from the appropriate final review office (see 3 FAM 4174.3(a)). They also must still adhere to the content limitations found in 3 FAM 4176.2 and must **not**:

- Claim to represent the Department or its policies, or those of the U.S. government;
- Use Department or other U.S. government seals or logos;
- Disclose, or in any way allow the public or any unauthorized person to access, classified or sensitive information, even if it is already publicly available due to a previous unauthorized disclosure; or
- Make publicly available or relay to any unauthorized person:
    - Material that meets one or more of the criteria for exemption from public disclosure under the Freedom of Information Act, 5 U.S.C. 552(b), including internal pre-decisional deliberative material;
    - Information that reasonably could be expected to interfere with law enforcement proceedings or operations;
    - Certain information pertaining to procurement;
    - Sensitive personally identifiable information as defined in 5 FAM 795.1(f); or
    - Other nonpublic information, when used in a manner as prohibited by 5 CFR 2635.703.

14. Employees should also remember that under 3 FAM 4177, "[f]ailure to follow the provisions of [3 FAM 4170], including failure to seek advance reviews where required, may result in disciplinary or other administrative action up to and including separation." Further, the review is not meant to insulate employees from discipline or other administrative action related to their communications. Ultimately, employees remain responsible for their personal capacity public communications whether or not such communications are on topics of Departmental concern (3 FAM 4174.2(c)).

Security Issues

15. In addition to the prohibition on disclosing sensitive, classified, and other protected nonpublic information discussed above, employees abroad may not transmit, publish, or stream live video or photographs from inside Post or Chief of Mission facilities without clearance from the Regional Security Officer (RSO), per established procedures for approved public events.

16. Engaging in online and digital activities can be a security risk. Posting information to personal social media accounts, or in messaging groups in any capacity or format, could allow ill-intentioned actors to leverage employees' information for malicious purposes, including coercion, intimidation, or embarrassment. It could also potentially expose employees to counterintelligence operations.

17. Department employees are encouraged to implement the strongest privacy and security settings offered for their personal social media accounts and to exercise caution when sharing information in messaging groups in order to prevent malicious actors from viewing or accessing their personal information. This does not ensure, however, that any information posted on these forums or others will either remain private or prevent others from seeking to gain leverage or influence over Department employees. More information and tips on securing personal social media accounts are available in the Bureau of Diplomatic Security (DS), Directorate of Cyber and Technology's (CTS) Cybersecurity Awareness Social Media Guide.

Ethics, Standards of Conduct, and Other Activity Limitations

18. Employees must ensure their personal social media activity complies with all Department policies and applicable ethics laws and regulations, including the Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635, and as outlined in 11 FAM 610. The Standards of Conduct prohibit employees from using their titles or positions in any manner that would create an appearance of official endorsement or sanction of their activities or opinions. Note that simply having "works at the Department of State" in one's personal social media profile does not preclude an employee from engaging in otherwise permissible activity on his or her personal social media platform, unless other circumstances (an official picture, etc.) make the profile appear official. Employees should not give the appearance of supporting any product or entity, policy, or outcome as an official representative of the U.S. government.

19. Among other things, the Standards of Conduct also prohibit a supervisor from ordering or asking a subordinate to work on the supervisor's personal social media account and, with a few exceptions, prohibit employees from receiving compensation for social media communications related to their official duties (11 FAM 614.5).

The Hatch Act and Political Activities

20. Department employees are generally permitted to express opinions about political topics on personal social media accounts so long as they do **not**:

- Claim to represent the Department or U.S. government when expressing those views;
- Disclose sensitive or classified information;
- Address matters of Departmental concern (or the employee seeks the appropriate advance review if they do); or
- Express themselves in a manner inconsistent with applicable Department rules, including the Hatch Act or the Department's guidance on political activities (see Refs B and C for further information).

Employees with questions about permissible political activities should write to ethicsattorneymailbox@state.gov.

Resources and Guidance

21. As a reminder, Department employees must adhere to all applicable policies and guidance when using their personal social media accounts and communicating on digital platforms. Detailed guidance and resources include (but are not limited to):

- 3 FAM 4120 - Employee Responsibilities Abroad
- 3 FAM 4170 - Review of Public Speaking, Teaching, Writing, and Media Engagement
- 5 FAM 790 - Using Social Media
- 10 FAM 180 - Official Communication Using Social Media
- 11 FAM 610 - Ethics and Financial Disclosure Programs
- 11 FAM 614 - Outside Activities and Political Activities
- Social Media Policy for Ambassadors (OpenNet, GO Browser)
- Transitioning Departing Principal Twitter Accounts (OpenNet, GO Browser)
- L's Ethics and Political Activities SharePoint Site
- Social Media Hub (OpenNet, GO Browser)
- Personal and Official Use Social Media Handbook (OpenNet, GO Browser)
- GTM/ER's Manager Support Unit SharePoint site; ManagerSupport@state.gov
- DS/CTS Cybersecurity Awareness Social Media Guide

22. This ALDAC is not intended to be exhaustive, but reminds employees of their responsibilities relating to personal social media use and digital platform communications. Employees are advised to review this ALDAC carefully and regularly revisit the guidance to ensure they are in compliance with Department policy and procedures. Failure to follow Department policies may result in a proposal for disciplinary action, up to and including separation.

Signature: Blinken