2-9 Social Media

Policy Type: Local
Responsible Office: Chief John Venuti, Virginia Commonwealth University Police Department
Initial Policy Approved: 1/01/2013
Current Revision Approved: 4/4/2017

General

The Department endorses the secure use of social media to enhance communication, collaboration, information exchange, streamline processes and foster productivity. The purpose of this policy is to establish the Department's position on the utility and management of social media and to provide guidance on its management, administration and oversight. This policy is not meant to address one particular form of social media; rather social media in general as advances in technology occur and new tools emerge. This policy is consistent with the provisions of the Department of Human Resource Management (DHRM) policy, pursuant to the authority provided in §2.2-1201 and Code of Virginia §2.1-2827. Refer to DHRM Policy 1.75 – Use of Electronic Communications and Social Media. Compliance with this policy ensures the appropriate, responsible, and safe use of electronic communications and social media by VCUPD employees.

Accountability Statement

All employees are expected to fully comply with the guidelines and timelines set forth in this written directive. Failure to comply will result in appropriate corrective action. Responsibility rests with the division commander to ensure that any violations of policy are investigated and appropriate training, counseling and/or disciplinary action is initiated.

General Requirements

Department employees enjoy free speech rights, but such rights are subject to certain limitations due to the nature of law enforcement work. It is the policy of the Virginia Commonwealth University Police Department to regulate social media activity that may adversely impact the Department overall, university, or its employees and mission. As such, this policy provides precautionary information, as well as specific prohibitions on the use of social media by Department personnel.
When using electronic communication tools and social media, users shall:

A. Follow all applicable Commonwealth policies. Users may not violate any provision of DHRM Policy 1.75 - Use of Electronic Communications and Social Media, Written Directive: 2-9 Social Media, or any other policy, regulation, law, or other guideline set forth by VCU rules, state or federal law (see Va. Code §2.2-2827). This may include, but is not limited to, copyright laws, trademark laws, and other legislative requirements.

B. Be responsible and professional in their electronic activities. Employees shall conduct themselves in a manner that supports the mission of the agency and the performance of their duties.

C. Exercise the appropriate care to protect the agency's electronic communication tools against the introduction of viruses, spyware, malware, or other harmful attacks. When using the Commonwealth's electronic communication tools, social media or Internet access, employees shall:
   1. Use the Internet, electronic communication tools and social media only in accordance with State and agency policy,
   2. Maintain the conditions of security (including safeguarding of passwords) under which they are granted access to such media, and
   3. Check with the appropriate agency staff prior to downloading or accessing a file or document if the source of the file or other circumstances raises doubts about its safety.

D. Be respectful of the agency/organization, other employees, customers, vendors, and others when posting and communicating information. Users should be sensitive to referring to or including others in their communications and posts, and should be aware of any potential associated liabilities.

E. Users shall obtain consent prior to communicating or posting information about the workplace.

F. The Chief's office shall maintain and monitor the Department's social networking accounts.
   1. The Chief's designee will manage all web applications in compliance with established State and University policies and protocols.
   2. No web application will be initiated or run in the name of the Department without the consent of the Chief of Police. No employee will post material on behalf of the Department without the expressed consent of the Chief of Police.
   3. Requests by Divisions or Units to utilize "social media" as a formal communications tool must be submitted to the Chief of Police or his designee for prior approval.
   4. Requests to develop project or program-specific uses for any social media tools should be directed to the Chief of Police or his designee for consultation and development. Consideration will be given to the appropriate venue and application of tools.
   5. The Chief of Police's designee(s), along with Public Affairs, shall routinely review social media accounts on a daily basis during the work week, as well as employ account settings and establish alerts regarding newly posted comments. They shall remove comments from the site if they are deemed obscene, offensive, or as directed by the Chief of Police, Public Affairs, or University Counsel.
6. Comments that attack or insult an individual or group, to include (but not limited to) name-calling, profanity, obscenity, defamation or remarks disparaging people on the basis of race, gender, sexual orientation, disability or national origin, will be removed from the Department’s sites.

7. The designee shall remove inappropriate comments from the webpage as soon as they are discovered. If feasible, they shall document by screen capture, remove the comment, log the date, time, user information and comment for future reference. If a particular user repeatedly posts inappropriate comments, the designee shall block that user from membership.

8. Social media content shall adhere to all applicable laws, regulations and policies, including all information technology and records management policies.

9. Social media content is subject to public records laws. Relevant record retention schedules apply to social media. Content must be managed, stored and retrieved to comply with open records laws and e-discovery laws and policies.

Business Use

When using electronic communication tools and social media, users should:

A. Use their accurate identities and state their affiliation when using electronic communications or social media for business purposes.

B. Ensure the security of sensitive or confidential information when communicating electronically or posting the information on internal or external websites, including social media.

C. Ensure information is accurate prior to posting on social media sites, state or agency websites, or other electronic media sites. If it is discovered that information is inaccurate after posting, users should work to quickly correct the errors.

Personal Use

When using electronic communication tools and social media for personal use, users shall be clear that their communication or posting is personal and is not a communication of the agency or the Commonwealth, including personal use outside of the work environment. For example:

A. Users shall use their personal email addresses, and not those related to their positions with the Commonwealth, when communicating or posting information for personal use.

B. Users may use a disclaimer when posting opinions or views for personal use, such as, “the views expressed on this (website, blog, social media site) are my own and do not reflect the views of my employer or Virginia Commonwealth University or the Commonwealth of Virginia,” when appropriate to ensure these views are not viewed as official agency communications.
Prohibited Activities

Certain activities are prohibited when using VCUPD, VCU or Commonwealth of Virginia's Internet and electronic communications media or using social media in reference to the work environment. Employees who engage in prohibited activities may be subject to disciplinary action, according to State Policy 1.60, Standards of Conduct. Prohibited activities include, but are not limited to:

A. Any use that is in violation of applicable local, state, and federal law.
B. Accessing, uploading, downloading, transmitting, printing, posting, or storing information with sexually explicit content as prohibited by law (see Va. Code §2.2-2827).
C. Accessing, uploading, downloading, transmitting, printing, posting, or storing fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images.
D. Installing or downloading computer software, programs, or executable files contrary to the Virginia Information Technology Agency's (VITA) Information Technology Resource Management (ITRM) Policies, Standards and Guidelines.
E. Accessing, uploading, downloading, transmitting, printing, communicating, or posting access-restricted agency information, proprietary agency information, sensitive state data or records, or copyrighted materials in violation of agency or state policy.
F. Using proprietary agency information, state data or records, and social media to locate agency customers for personal reasons.
G. Posting information or sending electronic communications, such as email using another's identity.
H. Permitting a non-user to use for purposes of communicating the message of a third-party individual or organization.
I. Posting photos, videos, or audio recordings taken in the work environment without written consent.
J. Using agency or organization logos without written consent.
K. Texting, emailing, or using hand-held electronic communications devices while operating a state vehicle according to the Office of Fleet Management Services Policies and Procedures Manual.
L. Any other activities designated as prohibited by VCUPD policy, such as:
   1. No photographs, facsimiles, drawings or other depictions of the Virginia Commonwealth University Police Department uniforms, badges, patches, seals, police vehicles/equipment or anything else that might visually represent the Department shall be used or published in a manner that would tend to bring discredit to the Department or any State or University employee. Employees appearing online in uniform automatically create a link between their online content and their employment with the Department.
   2. As public employees, all personnel are cautioned that speech made on or off-duty, pursuant to their official duties, that owes its existence to the employee’s professional duties and responsibilities, is not protected under the First Amendment and may form the basis for disciplinary action, up to termination, if deemed detrimental to the Department. Personnel should assume that their speech and related activity will reflect upon the Department.
3. Department members should be aware that privacy settings and social media sites are in constant flux. Employees should never assume that personal information posted on such sites is protected.

4. This policy supplements the directives for employee conduct contained in all other Department directives or policies, and provides guidance for employees in applying those standards to the content of their online postings. The following rules apply when publishing content online:
   a. Employees shall not post content that contains material that is inappropriate for public viewing, such as, but not limited to, content that promotes illegal activity, violates the rights of any person or entity, or threatens the safety of any person or entity.
   b. Engaging in prohibited speech noted herein, may provide grounds for undermining or impeaching an officer's testimony in criminal proceedings. Department employees thus sanctioned are subject to discipline up to and including termination.
   c. Posted content has the potential to be shared broadly, including to people with whom employees did not intend to communicate, and may be subpoenaed by opposing counsel if it is relevant to a lawsuit related to an employee's official duties. Employees shall keep in mind that all content may be printed and re-distributed outside of the original recipient group.
   d. Employees shall not engage in social networking activities on the Internet while on-duty, unless such use is part of an ongoing criminal investigation or other Department function. Use of social media tools remain subject to the University's computer use policies.
   e. Employees should expect that any information created, transmitted, downloaded, exchanged or discussed in a public online forum may be accessed by the Department without any prior notice.
   f. Any employee becoming aware of or having knowledge of a posting or of any website or webpage in violation of this policy, shall notify his or her supervisor immediately.

Issues of General or Public Concern

Employees may comment on issues of general or public concern, as opposed to personal grievances, including, but not limited to: local issues and criticism of local officials and policies, as long as the comments do not disrupt the workplace, interfere with important working relationships or efficient workflow, or undermine public confidence in the employee, the Department or the University. These instances shall be assessed on a case-by-case basis, as necessary. The employee shall adhere to the following guidelines, provided to assist in determining whether content is appropriate:

A. Matters of public concern are matters of interest to the community as a whole, whether for social, political or other reasons (see Va. Code § 15.2-1512.4).

B. Code of Virginia §15.2-1512.4 permits employees to express opinions on matters of public concern to state or local elected officials, regardless of the impact on the workplace.

C. Examples of local issues of general concern include: the budget, spending priorities, any question scheduled for public hearing, illegal discrimination, official corruption, official impropriety, malfeasance on the part of the government, misuse or waste of public funds, fraud, abuse or gross mismanagement, inefficiency in managing and operating government agencies, violation of law, local elections and/or public safety.
D. Examples of state or national issues of general or public concern include: election campaigns, elected officials, legislation, national security, budgets, foreign policy, and/or any topic of broad public interest and debate.

E. Examples of personal grievances that do not constitute issues of general or public concern, include: disciplinary action, work schedule, morale, and complaints about supervisors or co-workers that do not involve actual wrongdoing, illegal discrimination, corruption or waste. These comments may subject an employee to disciplinary action if they constitute insubordination or otherwise violate general rules governing an employee’s code of conduct.

Agency Responsibilities and Requirements

A. Monitoring Usage
   1. No user shall have any expectation of privacy in any message, file, image or data created, sent, retrieved, received, or posted in the use of the Commonwealth’s equipment and/or access. Agencies have the right to monitor any and all aspects of electronic communications and social media usage. Such monitoring may occur at any time, without notice, and without the user’s permission.
   2. In addition, except for exemptions under the Act, electronic records may be subject to the Freedom of Information Act (FOIA) and, therefore available for public distribution.

B. Communication
   1. Electronic records shall be retained in accordance with the record retention requirements set forth by the Library of Virginia.
   2. Acknowledgement statements, signed by each user, acknowledging receipt of a copy of University policy and DHRM Policy 1.75 - Use of Electronic Communications and Social Media, shall be signed and retained in accordance with the provisions set forth by the Library of Virginia.
   3. Violations of this policy must be addressed under State Policy 1.60 - Standards of Conduct, or appropriate disciplinary policy or procedures for employees not covered by the Virginia Personnel Act. The appropriate level of disciplinary action will be determined on a case-by-case basis by the agency head or designee, with sanctions up to or including termination, depending on the severity of the offense, as consistent with State Policy 1.60 or other applicable policy.

Revision History

This policy supersedes the following archived policies:

1/2013 2-9 Social Media