Chapter: 5	Effective Date:	Amends/Supersedes:	By Authority of the Chief of Police
Procedures	March 8, 2023	October 1, 2012 May 4, 2017	Charles A. Penn
Accreditation Standard(s): ADM.22.01			

519.02 Social Media

I. Policy

The department endorses the secure use of social media to enhance communication, collaboration, and information exchange; to streamline processes and advance productivity; and conduct criminal investigations. This policy, in addition to the County's Social Media Administrative Regulation and Administrative Regulation 2.7, establishes our department's position on the use and management of social media. Additionally, the policy will provide direction on the management, administration, and oversight of user-generated content. Social media platforms include, but are not limited to, social media sites such as Facebook and Twitter, web sites, blogs, and electronic communications, such as emails and texts from County owned devices. When utilizing social media to conduct criminal investigations, employees shall do so in an appropriate, ethical, and lawful manner that preserves the safety, privacy, and civil liberties of the individual or organization under investigation.

II. Definitions

A. Covert Online Account – Any account for a social media, messaging application, online forum, or other electronic communication platform that uses a false identity or in any way attempts to mask a user's identity and is created or used for any purpose related to the user's status as an employee of the Department.

B. Investigative Account – A Covert Online Account which may lead to interaction with other users.

C. Research Account – A Covert Online Account which will never include any form of interaction with other users.

III. Procedures

A. Department Sanctioned Social Media Sites

1. All Department social media sites, postings or pages must be approved by the Chief of Police or designee and will be administered by the Media Relations and Public Affairs Office or as otherwise determined.
2. Where possible, the page and/or site should link to the Department's or County's official website.

3. Where possible, each maintained social media site shall include a statement that clearly specifies the purpose, scope, and terms of use of the Department's presence.
4. Social media pages and/or sites shall clearly indicate that they are maintained by a designated Department member and shall have Department contact information displayed. The site or pages shall also be monitored by assigned Department personnel.
5. Social media site usernames and passwords will be created by the Media Relations and Public Affairs Office. The Public Information Officer will provide at least one additional Department employee with that information and keep that employee informed of any changes to log-on information. These usernames and passwords shall not be shared.
6. Social media content shall adhere to the established guidelines in the County's Social Media Policy.
7. Where possible, social media sites and/or pages should state that the opinions expressed by residents, businesses and visitors do not reflect the opinions of the Department or Arlington County, its Board or County Manager.
    a. Sites and/or pages should clearly indicate that posted comments will be monitored, and the Department reserves the right to remove any material, as it is a moderated online discussion site and not a public forum.
    b. Sites and/or pages should clearly indicate that any content posted or submitted is subject to public disclosure.
    c. Copies of any materials determined to be in violation of this policy will be removed from Department social media platforms and a copy retained by the Department for an appropriate period of time.

B. Social Medial Communication Requirements

1. Personnel representing the Department through social media outlets shall:
    a. Conduct themselves professionally at all times as a representative of the Department.
    b. Adhere to Department standards and policies.
    c. Identify themselves as an employee of the Department.
    d. Maintain confidentiality of "Law Enforcement Information." Law Enforcement Information shall not be shared with non-Department personnel, the public or on social media platforms without authorization. "Law Enforcement Information" includes photos, audio files or names of individuals arrested or persons of interest; cases under investigation or completed; evidence of crimes; crime scenes; seizures; undercover personnel or activities; police reports; confidential informant information; special operations; tactics; surveillance; security efforts

and other information that constitutes official law enforcement activities. This obligation also includes not expressing personal opinions or volunteering information about state, federal or local law enforcement activities.

e. Members authorized to work with the Department's social media platforms also should also not affiliate with, advocate for, or promote, any political party or private business.

f. Department personnel shall observe and abide by all copyright, trademark and logo restrictions when posting material within social media platforms.

C. Non-Department Social Media Platforms and Other Electronic Communications

1. This policy does not restrict personnel from commenting on issues of general or public concern (as opposed to personal grievances) so long as the comments do not disrupt the workforce, interfere with important working relationships or efficient workflow, impede investigations, or undermine public confidence in the employee or the Department. Compliance with this section will be considered on a case-by-case basis.

2. "Law Enforcement Information" is considered confidential, protected, controlled, or private and shall not be posted or referred to on private social media platforms or in private electronic communications.

3. Revealing confidential Law Enforcement Information without approval is strictly prohibited and may be subject to disciplinary action.

4. The use of the Department's seal, uniform, equipment, property, canines, or vehicles on private social media platforms should not be done in a manner that reflects conduct unbecoming, would undermine the public's trust in the Department and its personnel, that tarnishes or demeans the Department's core values or brings discredit upon the Department or its employees; or would otherwise suggest Department enforcement or promotion of private enterprises, events or political candidates.

5. As outlined in Directive 518.01 *Uniform*, personnel may not download, use, disseminate, publish, or copy the seal, markings, logo, or badge on any social media site for personal use without written permission from the Chief of Police or designee.

6. The Department reserves the right to review information created, transmitted, downloaded, exchanged, or discussed on social media platforms or other electronic communications when:

a. Posted in the public domain.

b. Brought to the attention of Department personnel and provided by employees or civilians.

c. Part of a criminal or internal affairs investigation.

7. Employees who believe they have been subject to inappropriate online conduct are encouraged to report the misconduct to the Office of Professional Responsibility. Employees who have witnessed prohibited online conduct should report the conduct to their chain of command.

D. Covert Online Accounts

1. Covert Online Accounts shall be used only for legitimate law enforcement purposes.
2. All Covert Online Accounts used by employees for official Department duties are owned exclusively by the Department.
3. For the purposes of this policy, the use of an existing online account belonging to a person involved in an investigation (e.g., victim, witness, reporting party, etc.) with the account owner's permission shall not be considered creating or using a Covert Online Account.
4. Before creating or using a Covert Online Account, an employee must demonstrate a valid reason for creating or using a Covert Online Account and receive approval from the Homeland Security Section (HSS) and the employee's chain of command up to and including their Division Commander. To request this approval, an employee must submit a Covert Online Account Application Form to HSS. HSS personnel will notify applicants when their application has been approved or rejected.
5. Approved Covert Online Accounts shall be assigned a unique identifier. This identifier will be recorded on the Social Media Application Form and provided to the applicant. All Social Media Application Forms will be stored electronically by HSS personnel.
6. Only employees who have completed training approved by HSS on the creation and use of Covert Online Accounts may create or use a Covert Online Account. Completion of such training shall be documented in the employee's Training record in LERMS.
7. Employees shall create and use Covert Online Accounts in accordance with Department-approved training.
8. A record of all usernames and passwords linked to Covert Online Accounts must be maintained by the employee and made available, upon request, to any supervisor in the employee's chain of command or the Office of Professional Responsibility.
9. Whenever a Covert Online Account is referenced in a Department document, the account shall be referenced by its unique identifier.
10. HSS shall conduct an annual audit of all Covert Online Accounts which, at a minimum, shall include contact with all employees who have approved Covert Online Accounts to determine whether each account is still in use. The results of the annual audit shall be shared with the chain of command for each employee with an approved Covert Online Account.

11. Covert Online Accounts may only be accessed or used on a device or equipment provided by the Department or another law-enforcement agency pursuant to a cooperative agreement.
12. Any Covert Online Accounts created or used by employees assigned as Task Force Officers at the behest of their respective task force agency shall follow that agency's policy regarding Covert Online Accounts.
13. Unless exigent circumstances exist, the use of any Covert Online Account shall be coordinated with the lead investigator of any related investigation or potentially related investigation.
14. The following activities are prohibited:
    a. Creating or using a Covert Online Account that purports to represent an actual juvenile or utilizes a photograph of an actual juvenile.
    b. Creating or using a Covert Online Account that purports to represent an actual or fictitious political figure, government official, or member of the press.
    c. Interacting or communicating in any way with other online users while using a Research Account.
15. The following activities require advanced written approval from a Section Commander:
    a. Creating or using a Covert Online Account that purports to represent an actual adult or utilizes a photograph of an actual adult. Officers wishing to create or use a Covert Online Account that purports to represent an actual adult or utilizes a photograph of an actual adult must also receive that person's advanced written consent.
    b. Creating or using a Covert Online Account that purports to represent a fictitious juvenile.
    c. Creating or using a Covert Online Account that utilizes any nude or sexually explicit pictures or images.
    d. The monetization of, or the sale and/or purchase of any goods from, a Covert Online Account.