



## TABLE OF CONTENTS

1. PURPOSE .....	2
2. SCOPE .....	2
3. AUTHORITY AND RELATED POLICIES .....	2
4. POLICY .....	3
5. GUIDELINES FOR EMPLOYEES.....	4
A. RESPECT OF DEPARTMENT TIME AND PROPERTY .....	4
B. CONFIDENTIAL INFORMATION .....	4
C. RESPECTFUL COMMUNICATIONS.....	4
D. QUESTIONS TO CONSIDER .....	5
E. USE OF EMAIL ADDRESSES ON SOCIAL NETWORKING SITES .....	5
F. REMEMBER YOU ARE RESPONSIBLE FOR WHAT YOU POST .....	5
G. DISCLAIMERS ON PERSONAL SITES.....	6
H. MONITORING .....	6
I. PRIVACY OF OTHERS .....	6
6. MODIFICATIONS .....	6
7. ENFORCEMENT .....	7
8. GUIDELINES FOR AFFILIATES HOSTING SOCIAL NETWORK SITES .....	7
A. DEVELOPMENT AND MAINTENANCE.....	7
B. POST ACCURATE INFORMATION .....	7
C. REMOVAL OF INAPPROPRIATE CONTENT.....	7
D. PUBLIC RECORDS.....	7
E. RETENTION OF RECORDS .....	7
F. COMMUNICATIONS AND PRIVACY EXPECTATIONS.....	8
9. COMPLIANCE.....	8
10. ATTACHMENTS.....	8
11. HISTORY NOTES.....	8
12. SIGNATURE.....	8



## 1. PURPOSE

The purpose of this policy is to establish guidelines for the use of social media and personal cell phones by the Department of Elder Affairs (hereinafter referred to as "Department") employees, contracted employees, consultants, OPS, and volunteers associated with the Department. This policy must be followed in conjunction with the Department's Management Information Systems Policy #420.10, Florida Administrative Code Rule chapter 60L-36: Conduct of Employees, and any other personnel policies regarding employee conduct. This policy is not meant to address any one particular form of social media and/or cellular communication; rather, it is meant to address social media and cellular communication in general since technology will outpace our ability to discover emerging means of communication and create policies governing its usage. Social media and means of cellular communication provide a valuable means of assisting the Department and its personnel in meeting community education, community information, and other related organizational and community objectives. This policy identifies possible uses that may be evaluated and utilized as deemed necessary by the Department administration.

The Department also recognizes the role social media and communication tools may play in the personal lives of Department personnel and employees. However, the personal use of social media and cellular communication can influence Department personnel in their official capacity. Therefore, this policy is intended to serve as a means to provide guidance of a precautionary nature as well as restrictions and prohibitions on the use of social media and other means of cellular communication by Department personnel.

## 2. SCOPE

This policy applies to employees, contracted employees, consultants, OPS, publicly created advisory boards, and volunteers, including all personnel affiliated with third parties that use the Department's computer resource systems. This policy also applies to the use of personal social media accounts and cellular or online transmission of any direct or incidental state business conducted through any electronic, internet, intranet, and/or wireless communication sent or received or accessed from both Department owned or leased devices and personal computers, cellular phones, personal digital assistants, smart watches, smart tablets, and other wireless communication devices.

## 3. AUTHORITY AND RELATED POLICIES

1. Title X, Public Officers, Employees and Records, chapter 119, Florida Statutes (2021);
2. Title XIX, Public Business, chapter 282, Florida Statutes (2021);
3. Florida Administrative Code Rule 60L-36.005, Disciplinary Standards;
4. Governor's Ethics Code 07-30-2019;
5. HIPAA Policies and Procedures;
6. Misuse of Access to Employee Records;
7. 310.20 Public Records Policy and Procedures;
8. 420.10 Department of Elder Affairs Management Information Systems Policy and Procedures;
9. 420.51 DOEA Information Security Policy;



10. 420.55 Printer Policy;
11. 545.10 Records Management Policy;
12. 545.11 Electronic Mail Policy;
13. 545.61 Wireless Communications Devices & Services;
14. 550.10 Standards of Conduct Chapter 60L-36;
15. 550.30 Code of Ethics;
16. 550.35 Conduct of Employees Disciplinary Guidelines;
17. 550.55 Sexual Harassment Policy; and
18. 550.95 Non-Discrimination on the Basis of Disability.

#### 4. POLICY

Social media is a term commonly used to describe websites and online tools which allow users to interact with each other by sharing information, opinions, knowledge, and interests. Social media and personal communication on social media platforms includes, but is not limited to social networking websites, blogs, podcasts, discussion forums, RSS feeds, video sharing, SMS (including Direct Messages or DMs, iMessages, wireless texts, etc.), social networks like Instagram, TikTok, Snapchat, Google Hangouts, WhatsApp, Signal, Facebook, Pinterest, and Twitter, as well as content sharing networks such as Flickr and YouTube.

The Department recognizes social media and various forms of electronic/cellular/online communication are powerful tools that may be used to enhance services, promote collaboration, provide information, and increase personal enrichment. The Department respects the rights of employees to use these tools as a medium of self-expression in their individual capacities. However, the Department also recognizes that permitting the use of such tools is not without risk and has developed the following guidelines employees must observe when using social media and cellular communication. The same high standards of conduct and behavior generally expected of government employees and public servants also apply when participating online through social media and in any interpersonal communication with the public via any means of electronic communication, including personal cell phones when conducting state business. All or any online participation by a Department employee should reflect and uphold the values, integrity, and reputation of the Department. Departmental employees have the same right to freedom of expression as other members of the community, subject to a legitimate public interest in maintaining an impartial and effective public service.

The Department's official electronic business is primarily conducted via the Department's email system and over communication devices, laptops, cell phones, etc. issued specifically by the Department. Therefore, if employees, contracted employees, consultants, OPS, publicly created advisory boards, and volunteers use social media and/or personal cellular communication including but not limited to texts, iMessages, Direct Messages (DMs), etc. to conduct official Department business, they must acknowledge their communications may be subject to the public records law in Florida. They must also provide notice to the public that all communications may be subject to Florida's public records law. This includes content posted on an organization's or entity's page, as well as information about the organization's or entity's friends list, followers, subscribers, etc. - all of which may be disclosed pursuant to chapter 119, Fla. Stat. (2021).



All Department personnel are strongly discouraged from using their Department email address and cell phones/direct lines for any personal emails and/or communication, as required by the DOEA Electronic Mail Policy #545.11. If so used, they will imply their consent to their personal information being a public record, open for disclosure to the public and to the Department of Elder Affairs' Administration. Furthermore, doing so may subject them to disciplinary action by the Department. If any Department personnel conducts any state business on their personal email or cell phone, they may be required to surrender all requisite related records of such conduct to the Office of the General Counsel for review pursuant to the public records law.

Department employees are not authorized to speak on behalf of the Department unless specifically authorized to do so in their role which is generally limited to staff in Communications who report to the Director of Communications and manage the Department's official social media accounts.

## **5. GUIDELINES FOR EMPLOYEES**

### **A. RESPECT OF DEPARTMENT TIME AND PROPERTY**

Use of Department computers and other wireless communication devices are designed and intended to assist the employee in the accomplishment of the employee's job assignments. Social networking must not interfere with the employee's timely performance of work obligations. Reasonable use of social media for personal use is permitted during breaks and lunch. Excessive use of social media during work hours is prohibited and may be grounds for disciplinary action as provided in Florida Administrative Code Rule chapter 60L-36.

### **B. CONFIDENTIAL INFORMATION**

Employees are prohibited from posting any confidential, proprietary, copyrighted, protected health information (PHI) or otherwise legally protected information/ materials on their social networking accounts. Employees are also strictly prohibited from posting, sharing, or discussing any of the aforementioned information on or through their personal cellular phone or any other means of personal communication. Improper sharing of any such information will render any employee subject to disciplinary action by the Department.

### **C. RESPECTFUL COMMUNICATIONS**

State Employees must remember to conduct themselves, on and off the job, in a manner that will not discredit or embarrass the state, its employees, or agents. This includes online activity and operation of social media accounts. Be respectful when using social media especially in communications and blogs related to or referencing the Department, an affiliate, or partner. Information exchanged on social networking sites can be accessed by vendors, suppliers, and business partners and can be kept online, in theory, forever.

1. Employees are prohibited from using social networking accounts to harass, bully, threaten, libel, slander, malign, defame, disparage, or discriminate against co-workers, managers, vendors, or anyone else. Behaviors that constitute harassment and bullying include, but are not limited to, comments that are derogatory with respect to race, religion, gender, sexual orientation, color, age, or disability; sexually explicit or



- suggestive, humiliating, or demeaning comments; and threats to stalk, haze, or physically injure another employee.
2. All employees including supervisors, managers, and administrators are cautioned to remember that if they "friend" or "follow" or "subscribe" to other employees, or subordinates, or subordinates of other supervisors, managers, and administrators on any social media platform, they need to maintain the same appropriate professional relationship online as in the office.
  3. Employees are prohibited from writing about, posting pictures of, or otherwise referring to any other employees without their permission.
  4. Employees should refrain from using profane and vulgar language and avoid discussions of conduct that is prohibited by Department policies, such as alcohol or drug use on state property or during work hours.

#### **D. QUESTIONS TO CONSIDER**

When considering making personal comments, employees should ask themselves the following questions:

1. Could your communication and/or comment cause the public and/or the Department's clients to lose confidence in your ability to work in an impartial and professional manner?
2. Is your communication and/or comment consistent with how the public expects the Department to operate and behave?
3. Could your comment lower or undermine the reputation of the Department?
4. Is your communication and/or comment lawful? For example, does it comply with anti-discrimination legislation and laws relating to defamation? Further, does it violate any ethics code and/or a public records law?
5. Would you be comfortable if your Supervisor/Manager viewed your communication and/or comment?
6. What if someone takes a screenshot of your communication and/or comment and then circulates it publicly? Would you be comfortable defending such a communication or comment?

#### **E. USE OF EMAIL ADDRESSES ON SOCIAL NETWORKING SITES**

Department email addresses must only be used for work-related communications and not for any personal social networking accounts or communications. The "elderaffairs.org" address attached to your name implies that you are acting on the Department's behalf and all actions are public and subject to public records laws. Please note that using a Department email address for any social media website or platform including making an Apple ID would render the entire social media account as potentially subject to the public records law.

#### **F. REMEMBER YOU ARE RESPONSIBLE FOR WHAT YOU POST**

You are responsible for any of your online activity conducted either on your own computer or with a Department email address, and/or which can be traced back to the Department's domain, and/or which uses Department assets, networks, and resources. Employees are prohibited from posting on any networking or internet site any photographs, video, or audio recordings taken on department property and/or in the performance of official duties



(including all official department training, activities, or work specific assignments) that are detrimental to the mission and functions of the Department, undermine respect or public confidence in the department, cause embarrassment to the Department, discredit the Department or its employees, or undermine the goals and mission of the Department.

1. Employees have no legitimate expectation of privacy for any personal communication or information sent or received via the Department's email address and/or network or network devices.
2. Department personnel should expect any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the Department at any time without prior notice.

#### **G. DISCLAIMERS ON PERSONAL SITES**

If you identify yourself as an employee of the Department, please remember to identify your personal views and opinions as your own in your individual capacity. You must note and make known that any such personal views expressed are your own and do not in any way represent the Department.

#### **H. MONITORING**

In conjunction with the Department's Management Information Systems Policy #420.10, the Department reserves the right, at its discretion, to review any employee's electronic files, messages, and usage to the extent necessary to ensure that electronic media and services are being used in compliance with the law and with this and other Department policies.

1. Employees must understand that anything they post online from any computer is public and employees should not assume they have a right to privacy with regards to electronic communications sent, received, created, accessed, obtained, viewed, or stored on the Department's systems.
2. As a matter of policy, however, the Department will not systematically monitor an employee's use of social media unless it is necessary for non-investigatory, work-related purposes, or for investigations of allegations of work-related misconduct.

#### **I. PRIVACY OF OTHERS**

Personal information about individuals cannot be provided to third parties without their consent. The email address of your colleagues or other employees/vendors and other identifiable information must be treated with discretion and care. Employees must not upload contact details from departmental (Outlook) contacts when using or prompted by external social networking sites. Also, department employees must not schedule personal appointments or meetings with other state employees using their outlook calendar or department email or communication tools.

### **6. MODIFICATIONS**

The Department reserves the right to modify, discontinue, or replace the policy or any terms of the policy. The Department will endeavor to give notice of all changes to its Social Media Policy.



## **7. ENFORCEMENT**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including dismissal, as provided by Florida Administrative Code Rule 60L-36.005.

## **8. GUIDELINES FOR AFFILIATES HOSTING SOCIAL NETWORK SITES**

This policy applies to any organization or entity affiliated with the Department of Elder Affairs that chooses to maintain a social networking service using the Department's computer resource systems. Please remember that the Department's official electronic business is primarily conducted via the Department's email system and not through social media.

### **A. DEVELOPMENT AND MAINTENANCE**

Organizations or entities affiliated with the Department must use good judgment and professionalism when creating and maintaining a social networking page. Be cognizant that what is posted by the organization reflects on the Department.

### **B. POST ACCURATE INFORMATION**

The organization or entity must post accurate information and promptly correct any misinformation posted.

### **C. REMOVAL OF INAPPROPRIATE CONTENT**

The organization must be responsible for screening and removing content that is offensive, rude, discriminatory, vulgar, libelous, slanderous, or in any other respect in violation of the Department's policies or its contracts.

### **D. PUBLIC RECORDS**

All content on the organization's or entity's page, including information about the organization's friend list, followers, subscribers, and messages (sent and/or received), are subject to disclosure under the Florida Public Records Act. Therefore, the organization or entity must post a notice to the public that all communications may be subject to Florida's public records law. This includes content posted on an organization's or entity's page, as well as the information aforementioned, all of which may be disclosed pursuant to chapter 119, Fla. Stat. (2021). If a new public record is created, its content must be maintained per its specific retention schedule. Input received on a policy or service must be saved and kept per its retention schedule. Refer to the Department's Records Management and Archival Policy #545.10 for detailed information regarding records maintenance and handling.

### **E. RETENTION OF RECORDS**

The organization or entity is required to have the capacity to electronically archive or store all communications sent or received on social networking sites that involve Department business. Entities must follow the records retention schedule as set forth in the Florida Department of State's General Records Schedule for State and Local Government Agencies (GS1-SL). The Department's Information Technology Personnel are available to assist with electronic storage space, if needed. Information that provides evidence of



business activity or decision is a public record. All Department employees have an obligation to ensure that key decisions and events are recorded in a way that captures the important features of a discussion or decision, presents a faithful and accurate account, and can be easily retrieved when needed. Social media platforms are often provided by third-party providers and are not official recordkeeping systems. In managing content in the Department's social media accounts, you must keep records in accordance with the Public Records Policy and Procedures #310.20, ensuring appropriate records are created and captured for all the business functions, activities, and transactions. Employees are required to appropriately classify and store information as set out in the Department's Records Management and Archival Policy #545.10.

#### **F. COMMUNICATIONS AND PRIVACY EXPECTATIONS**

Any communications on any social networking site regarding Department business is subject to Florida's Government in the Sunshine Law. For example, members of a council, board, or commission may not engage on any social networking site in a discussion of matters that foreseeably will come before the council, board, or committee for official action.

In accordance with Florida's public records law, the public may request information made or received by the Department employees in the performance of their jobs. Therefore, employees must consider all information, including social media postings, open to public view. Additionally, employees must comply with all records retention regulations when posting to social networking forums and sites.

### **9. COMPLIANCE**

All Department employees must comply with this policy. Failure to abide by the policies set forth herein may subject the Department, its employees and contract staff to serious civil and/or criminal liability. Failure to comply with this policy may also result in disciplinary sanctions, as provided by Florida Administrative Code Rule 60L-36.005, including dismissal from employment or contract termination.

### **10. ATTACHMENTS**

1. DOEA Policy #340.35 Social Media & Personal Cell Phone Use Policy Acknowledgement Form (Attachment A)

### **11. HISTORY NOTES**

New 08/23/2010;  
Substantially Revised 7/12/2021.

### **12. SIGNATURE**

Secretary: 

Effective Date: 8/2/2021





**Attachment A**

**ACKNOWLEDGEMENT FORM**

**DOEA Policy #340.35, *Social Media & Personal Cell Phone Use Policy***

I understand it is my responsibility to review this document and request any necessary clarification from my supervisor. I acknowledge that my failure to comply with DOEA Policy #340.35, *Social Media & Personal Cell Phone Use Policy* may result in disciplinary action, up to and including dismissal. I have read and understand the provisions DOEA Policy #340.35, *Social Media & Personal Cell Phone Use Policy*. I also understand that this signed acknowledgement of receipt will become a permanent part of my personnel file. I acknowledge that if I conduct state business on my personal email or cell phone, I will, upon request, surrender all requisite related records of such conduct to the Office of the General Counsel for review pursuant to the public records law.

Typed or Printed Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_