Policy

Policy Title:	Social Media				
Policy Number:	DHS-120-004	Version:	1.0	Effective Date:	07/11/2012

Approved by Jim Scherzinger
Chief Operating Officer

07/11/2012
Date approved

Overview

Description: Social media includes various online technology tools that enable people to communicate easily via the internet to share information and resources. Commonly used social media tools such as Facebook©, Google+, Twitter©, MySpace™, Skype™, YouTube©, and various mobile applications are important outreach and communication tools. These tools can encompass audio, video, images, podcasts, and other multimedia communications. When used properly, social media can facilitate networking and relationships between people, encourage new ideas, and convey information.

Social media accounts may be used to engage the public in conversations about our department, programs and to promote events. As part of our work, social media may be used for research and investigation helping program staff stay in touch with populations they serve and examine behaviors of our clients who may be at risk. Social media can also be used for education, training and job and volunteer recruitment.

Purpose/rationale: The intent of this policy is to cover expectations concerning the use of social media. DHS expects use of social media to be representative of the department's values and goals. Social media must be used thoughtfully and in a manner that minimizes risk to the department, employees, volunteers, contractors, agents and clients. Information is expected to be reliable and accurate. Use will not compromise the privacy of clients, individuals, or proprietary information such as network IP addresses or computer passwords. This policy applies to the work of the department but may also apply to personal use of social media that may affect work.

Applicability: All DHS employees, volunteers, contractors, agents, trainees, and interns.

Failure to comply: Failure to comply with this policy may result in disciplinary action up to and including dismissal. Legal action also may be taken for violations of applicable regulations and laws.

Policy

1. General

a. Public-facing use. The Office of Communications manages the public-facing use of social media including facilitating public comments. Authorization is required before creating or posting information on social media tools on behalf of the department. The Office of Communications can guide you through this process. They review the intended purpose and content of the site and manage the tracking of accounts.

b. Investigative use. Programs manage program-related use for activities such as research, investigations, and peer or professional collaboration that do not require the creation of a public-facing account. Some platforms, such as Facebook, require a public-facing account to use it appropriately. Both program and the Office of Communications should be consulted in this case.

c. Stakeholders. The Office of Communications and Program Offices will consult with stakeholder groups regarding the use and management of social media to determine and evaluate the impact or risk to the organization. Stakeholder groups may include:

   A. Executive Management
   B. Program areas
   C. Information Security and Privacy Office
   D. Human Resources
   E. Office of Information Services

d. Workplace impact. Use of social media is subject to all applicable policies, rules, and regulations.

2. Acceptable Use

a. Follow agency policies concerning confidential information. For example, if you post on the Facebook wall of a client you may be compromising their confidentially since that information is generally shared with all of their friends.

b. Follow the *Maintaining a Professional Workplace* policy which covers derogatory, offensive, discriminatory, threatening, harassing or otherwise unprofessional comments.

c. Public records retention requirements apply to all information posted on social media sites. Most social media tools do not retain records according to state requirements. You are responsible for retaining an official copy of the information posted by you and your visitors. This can be accomplished through a screen print saved to your shared computer drive.

d. Create specific social media business sites separate from personal accounts. Some social media tools don't allow this (i.e. Facebook). Consult with the Office of Communications for more information.

e. Accounts that conceal your identity through pseudo names or aliases are generally not allowed. Consult with your program manager if you have an investigative need.

f. Initial client contact via social media e-mail or instant messaging may be appropriate but you must direct any on-going continuing conversations back to your official work e-mail or other agency approved communication channel.

3. Account Management

a. An account administrator and at least one designated backup must be assigned to maintain the site content and settings. Special attention must be given to the privacy and security settings, terms of service and rules of conduct within the social media application. These settings are subject to frequent changes without notification. It is the

administrators' responsibility to review them regularly.

b. An account password must be changed immediately whenever there is a change in account administrators (this includes when an employee leaves employment at DHS).
c. Accounts must be removed or deleted when the site is no longer active. The Office of Communications must be notified when a public-facing account is deactivated.
d. The Office of Communications will maintain a current list of public-facing social media sites and the administrators of those accounts.
e. Administration of accounts must be performed on an agency computer or through approved agency remote access systems (Citrix or VPN).

4. Content

This section applies specifically to public-facing social networking as part of your job duties.

a. Consult with the Office of Communications in developing your message when representing the agency. Follow agency writing and style guidelines.
b. Establish a process to edit and review content changes to ensure that the information you post is accurate, professional, and up to date.
c. Each public-facing social media site must contain contact information to include agency address, telephone number, e-mail, and official Web sites.
d. If the content is open to public comment a moderator(s) must be assigned. The moderator is responsible to monitor postings daily for offensive or off-topic comments.
e. When applicable, post an acceptable use statement for visitors to your site defining appropriate content. Include expectations or rules of conduct for appropriate behavior and posting of comments. The Office of Communications has examples and can help you develop your statement. The Office must approve the acceptable use statement.
f. Quickly correct misinformation.
g. Pictures, videos, and sound recordings of clients can only be used on social media sites that are governed by DHS or OHA if a Media Release/Consent form (DHS/OHA 2130 Adults, DHS/OHA 2131 Minors) is completed.
h. Posting of content on social media sites shall comply with copyrights, license, contracts, intellectual property rights and laws associated with data, software programs, and other materials made available through those systems. See: DAS *Acceptable Use of State Information Assets*.

5. Information Security

a. Access may be blocked to social media tools that present an unacceptable level of risk to the agency or by business decision.
b. Users of social media must be aware of scams and viruses. Social media tools generally contain third-party content not under the control of the agency. Malicious code may be hidden in links, games, surveys, advertisements, e-mail, and instant messaging programs. It is recommended that you do not click on or follow links to third-party content displayed on social networking pages.
c. If you use your personal computer or other information resources to perform any job duties (i.e., to telework), and in the event of litigation, your computer may be subject to seizure and examination. State information stored on personal electronic equipment may be subject to agency review, public records requests, and discovery. See: *DAS Telecommuting and Teleworking* policy.
d. Use of social media on state owned equipment is monitored for appropriate use.
e. Passwords used in the administration of social media sites must differ from agency

passwords (examples: network password, RACF password, case management system password). For guidance, follow the agency *Password and User Identification Security* policy.

f. In accordance with the *Statewide Acceptable Use of State Information Assets* policy, do not use social media applications such as chat windows, or games provided within the social media application on work computers or electronic devices provided by the agency.
g. All information posted to social media sites should be *Level 1 classification "Published" only* as specified in the *Statewide Information Asset Classification* policy.
    A. Do not post or share confidential or personally identifying information about clients or co-workers. Examples include, but are not limited to, names in connection with medical or financial records, Social Security numbers, case/account numbers, addresses, e-mail, and phone numbers.
h. If you insert hyperlinks to external sites in your social networking media content, you may NOT use shortened URLs or a URL shortening service (TinyURL, Bitly, Goo.gl). You must display the entire link in your post for security, transparency, and ease of use.
    A. Shortened URLs are a popular method of introducing viruses and malware to unsuspecting visitors. Do not click on a shortened URL posted at a site you visit unless you are able to preview the actual web address that it is masking.
i. Log out of your account or close your browser window when you are finished viewing, posting, or administering a social media site. Many social media tools automatically and continuously refresh your page every few seconds which can slow down network availability.

6. Personal use of social media affecting state business

a. Some clients may find employees when social networking. We encourage employees to periodically review privacy settings on their personal social media accounts. This will help prevent conflicts of interest and privacy or confidentiality violations for our clients.
b. Relationships with clients on your personal social media site may constitute a breach of privacy or violate other policy and law. Refer to the *Conflict of Interest* policy.
c. When expressing yourself as an individual about matters of public concern, you should not imply that your personal opinion reflects the views of state government or the department unless authorized to speak on behalf of the agency.
d. Your personal or private social networking may impact the workplace if comments, posts, or sharing of information are threatening, harassing, or discriminatory towards co-workers, managers, partners of DHS/OHA and clients. This type of activity may violate existing state policies and Oregon/Federal laws.
e. Personal use of social media during work time is allowed only as specified in the *Acceptable Use of Information-related Technology* policy.

7. Prohibited Uses

The following actions are prohibited while using state owned equipment or resources or when the employee is on duty:

a. Posting or conveying of derogatory, offensive, discriminatory, threatening, harassing or otherwise unprofessional comments.
b. Personal solicitation of commerce.
c. Installing or using third party applications, games, surveys, e-mail, or instant

messaging on, or contained within, social media sites
d. Using aliases or fake accounts.
e. Posting or using information that may compromise the safety or security of the public, clients, or employees.
f. Engaging in illegal activity.
g. Conducting public meetings as defined by Oregon's public meeting law where deliberations or decision-making must occur in the open.

8. Exceptions

a. Exceptions may be granted on a case-by-case basis. Check with your manager.

Policies that apply:

DHS-010-005 Non-Discrimination on Basis of Disability
DHS-010-011 Acceptable Use of State Information Assets
DHS-020-006 Wireless Communication Devices
DHS-060-002: Conflict of Interest
DHS-060-013 Discrimination and Harassment Free Workplace
DHS 060-037 Use of State Property
DHS 060 038 Maintaining a Professional Workplace
DHS 070 004 Acceptable Use of Information-related Technology
DHS-070-005 Personal Digital Assistant (PDA)
DHS-070-010 Instant Messaging
DHS-090-002 Password and User Identification Security
DHS-090-003 Information Access Control Security
DHS-090-009 Computer Desktop/Laptop Security
DHS-100-001 DHS General Privacy Policy
DHS-120-003 Sensitive Issues

DAS 50.050.01 Statewide Policy: Telecommuting and Teleworking
DAS 107-004-0505 Statewide Policy: Information Asset Classification
DAS 107-004-110 Statewide Policy: Acceptable Use of State Information Assets

Forms that apply:

DHS-2130: DHS Media Release/Consent Form – Adults only
DHS-2131: DHS Media Release/Consent Form – for Minors

HS-2130 English: OHA Media Release/Consent Form – Adults only
HS-2130 Spanish: OHA Media Release/Consent Form – Adults only
HS -2131 English: OHA Media Release/Consent Form – for Minors
HS -2131 Spanish: OHA Media Release/Consent Form – for Minors

Definitions:

Social Media include various online technology tools that enable people to communicate easily via the internet to share information and resources.

Social Media Tools is the technology. Commonly used social media tools include Facebook©, Twitter©, MySpace™, YouTube©, LinkedIn®

Social Media Applications include add-ons to social media tools. These are the tools inside of social media tools. For example, Facebook© offers a chat window.

Social Networking is the collaboration. This is most commonly done by grouping individuals into specific groups. Though you can do many things with social media (like 1:1 interactions and mass communications) it's real and unique value is collaboration. Social networking is possible in person but in this context we are referring to online social networking.

Social Media Sites in this context refer to those pages built using social media tools.

Account or site administrator has access to the proper permissions and control over a social networking media.

Personally identifiable information - Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

References:

State Guidelines: Social Networking Media DAS
ORS Chapter 192.610 to 192.690 Records; Public Reports and Meetings

Contact:

Name: Jodi Sherwood **Phone:** (503) 385-7403 **E-mail:** jodi.sherwood@state.or.us

Policy History:

- **Version 1.0:**
  07/11/2012: Approved
  August 2012: Initial Release