STATE OF WASHINGTON
DEPARTMENT OF ARCHAEOLOGY & HISTORIC PRESERVATION
Protect the Past. Shape the Future

Social Media Networking Policy

Effective December 1, 2014

Approved by

Allyson Brooks, Director, State Historic Preservation Officer

Purpose

This policy is to define and establish the appropriate use of social media in the workplace.

Definitions

Social media or social networking – This refers to the use of the Internet for blogging, microblogging, media sharing, photo sharing, video sharing, wikis, discussion boards, and social networking. Social media includes text, images, audio, and video. Some examples of social media are:

- Blogs, and micro-blogs such as WordPress and Twitter.
- Social networks, such as Facebook and MySpace.
- Professional networks, such as Linkedin.
- Video sharing, such as YouTube and vlogs (video weblogs).
- Audio sharing, such as podcasts.
- Photo sharing, such as Flickr and Photobucket.
- Social bookmarking, such as Digg and Delicious.

Permitted Use

Staff may use social media only for approved agency purposes and to maintain the agency Facebook page, or any other social media outlet that is specific to the mission of the agency, including professional networking. Use of social media for personal purposes is not permitted on the **DAHP** equipment.

Staff may post appropriate material to DAHP social media sites or networks. Appropriate material may include text, images, audio, or video that supports or relates to the DAHP mission, cultural resource management, historic preservation practice, and/or other closely related fields. Any questions about appropriate material to be posted should be directed to the Director or Assistant Director.

Social media shall not be used to transmit information or knowingly connect to sites for an unlawful, unethical or prohibited purpose, including, but not limited to the following examples:

- Discrimination on the basis of sex, race, creed, color, gender, religion, age, marital status, national origin, sensory, mental or physical disability, sexual orientation, veteran status or genetic information.
- Transmission of obscene, defamatory, profane or otherwise offensive or inappropriate language or materials.
- Personal attacks, threats, sexual harassment or sites containing sexual content.
- Transmission of privileged, protected, confidential or private information.

- Transmission of proprietary information, copyright infringement or any infringement on intellectual property.
- Expression of any campaign, political or religious beliefs.
- Conduct of a personal, outside business or other financial benefit or gain.

Agency management has the authority to monitor employee use of the Internet on state equipment to ensure use is consistent with this policy.

Privacy Issues

Employees should have no expectation of privacy in the use of Internet resources. Employees using social media should never disclose privileged, protected, confidential or private information.

Owners of social media sites often share user activity and demographic information with third parties. This information may be captured directly during user interactions or indirectly using tracking cookies. It is important to remember that all activity conducted on social media sites is open to unrestricted public observation and users should conduct themselves accordingly.

The Internet is an unsecured publicly accessible network. Links and embedded files on social networking sites may contain malicious software or redirect users to inappropriate sites. Owners of social media sites commonly monitor usage activity and those activities may be disclosed to any number of parties.

Public Records

A record is defined broadly to include electronic records, those posted to or received by social networking websites. Any record that is prepared, owned, used or maintained by DAHP potentially relates to the conduct of government.

DAHP records posted to social media websites are not the primary record and are simply secondary copies governed by GS50001: "Administrative Material with No Retention Value."

Consequences and Restrictions

Failure to follow this policy for using social media or participation in inappropriate use of social media may result in the loss of access privileges and corrective or disciplinary action up to and including termination.

Primary roles and responsibilities for Social Media/Networking within DAHP.

Role	Responsibilities
Employee	Read, acknowledge with signature, and follow the policy for Social Media/Networking.
Supervisor/ Manager	Ensure that the policy for Social Media/Networking is read and followed.
DES HR Consultant	Answer any concerns and provide direction to the small agencies if situations arise.

WAC's and References that apply to this policy

- RCW 42.52.160 (ethics in public service)
- RCW 42.52.180 (use of public resources)
- WAC 292.110.010 (use of state resources)
- RCW 42.56 (Public Records Act)