

SAN LUIS OBISPO COUNTY

SOCIAL MEDIA POLICY

I. PURPOSE

This document describes the policy which governs employee participation in social media on behalf of the County of San Luis Obispo, including such topics as department approval, account management, acceptable use, employee responsibilities, content management, security, and public records retention.

Social media comprise the variety of web technologies that enable interactive and highly accessible communication. Examples of these technologies are often categorized under "Web 2.0" and include such services as Twitter, Facebook, StumbleUpon, YouTube, and LinkedIn along with blogs and wikis.

The use of social media presents a unique opportunity for county departments to connect with the public using instantaneous, interactive communication channels. These channels increase County and department responsiveness, improve information sharing, and facilitate greater public interaction with local government. However, along with these benefits, department heads and employees should also be aware of the risks involved.

II. SCOPE

This policy applies to all county employees, vendors or volunteers who use social media on behalf of the County or their department. It only applies to the use of social media interactions outside the County's Intranet.

This policy does not describe which social media services have been approved for use by county employees who participate in social media on behalf of the County. For a list of approved social media services, see [Social Media](#).

III. POLICY

When using social media for county-related purposes, employees must be aware of certain requirements, limitations, and guidelines that will ensure that their use of social media promotes the County's mission and is consistent with county values for professionalism, integrity, accountability, collaboration, and responsiveness. At the same time, maintaining credibility and security are key factors for the successful use of social media.

A. Department Approval

1. Each department wishing to participate in social media must review the list of approved services to identify which social media will best meet its goals. Please see [Social Media](#).
2. Only county employees, vendors or volunteers who are authorized by their department head may engage in social media on behalf of their department. For the purpose of this policy only, “county employee”, is synonymous with the definition of “User” in the Definitions section of the Information Security Policies and includes vendors and volunteers.
3. The department head must approve an employee’s use of the selected social media using the [Social Media Approval Form](#) or similar document as approved by County Human Resources.
4. The department head is responsible for approving the log-in account to be used for a social media site. This account is also documented in the Social Media Approval Form.

B. Account Management

1. Employees’ user names and passwords used to log into other county computing assets must not be used as the user name and password to log into a social media site. A generic county email account should be used when creating the social media account, such as “planning@co.slo.ca.us.” This will allow the generic account to be used by more than one authorized employee, and employee email accounts will not be exposed in public forums. This is especially important since most employee email accounts also contain the employee’s county network user name.
The password used to log into a social media account must *at a minimum* conform to the Password and Authentication Policy included in the [Information Security Program Policies](#) (under “Policies”). However, it is highly recommended that the length of the password used to log into social media accounts be longer than the existing Policies require because employees are logging into non-county, publicly accessible services. When using social media, it is recommended that the password should be at least 14 characters in length and incorporate upper and lower case letters, numbers, and special characters.
To test the strength of a password, see the Microsoft Safety and Security Center [password checker](#).
2. Department heads are responsible for maintaining the information for all social media accounts used by employees to represent the department. The information should include:

- a. Account information such as information needed to recover the user name or password (“secret question”), and the social media service or web site address associated with the account.
 - b. The names of employees who have access to or who use the account.
3. Departmental social media accounts must not be associated with a personal or private social media account. This will assist employees in keeping their personal social media separate from the social media they manage on behalf of their department.
4. Employee email addresses must not be used in contact information displayed in social media. Instead, links back to the county web site should be provided. If emailed responses from the public are required, provide a generic email account (such as “planning@co.slo.ca.us”).
5. Department heads must ensure that social media log-in accounts are modified when employees leave the department, no longer have authorization to engage in social media on behalf of their department, or when it is determined that there has been unauthorized use or access to the account.

C. Acceptable Use of Social Media

1. This policy does not supersede county policy regarding the use of county computing assets which are defined in the Information Security Program Policies. If in doubt regarding the use of county computing assets to participate in social media, consult your department head and the [Information Security Program Policies](#) (see the Acceptable Use Policy under “Policies”).
2. Departmental participation in social media is intended to promote communication with the public and to increase the transparency of local government. However, it is not intended to replace established channels of communication and public participation. [The Brown Act](#) (“Open Meeting Law”) specifies that meetings of public bodies must be open to attendance and participation by the public.
 - a. Employees must not make statements in social media or take actions resulting from their engagement in social media that circumvent or replace the public governance process or which violate the Brown Act.
3. Departmental and personal use of social media must be kept separate by adhering to the following:
 - a. Employees must not use their departmental social media account to engage in private or personal communication.
 - b. Employees must not use their personal social media account to engage in communication on behalf of the department or County.

4. Unauthorized use of social media on behalf of a department or the County may result in disciplinary action. Use of social media on behalf of a department or the County that violates County standards of conduct or otherwise violates this policy may result in disciplinary action.

D. Employee Responsibilities

1. Employees must comply with departmental guidelines for limitations on what content may be provided in social media and on the amount of time or level of interaction with which they may engage in social media on behalf of the department. For examples of the type of information which must not be communicated, see the "Content Management" section below.
2. Department heads are responsible for establishing the frequency with which employees may engage in social media on behalf of the department, such as daily or weekly. This frequency may be documented in the Social Media Approval Form or the department's equivalent approval form.
3. Employees representing their department or the County must not engage in social media in a manner that violates the County's mission, vision, and values statement; Human Resources policies or the department's policies governing employee conduct; federal, state, and local laws, rules and regulations; or the County's Acceptable Use Policy (see "Policies").
4. Employees must remain objective, respectful, and professional when interacting with the public using social media on behalf of their department or the County as outlined in the County Organizational Values.
5. Employees should attribute their social media communication to their department and when appropriate provide a link back to the county web site for further information. For elected or similar county officials, it may be more desirable to indicate the employee name and title to promote credibility and association of the content with the role of the person providing the content; for example, a blog from a Board Supervisor or the County Administrative Officer.

E. Content Management

1. Employees must not communicate confidential information in social media. This includes but is not limited to personnel, medical, law and justice, personally identifiable information (PII), and other sensitive, confidential, or privileged information. For more information, please see the definition of PII in the Sections Common to All Policies in "Policies" under the Information Security Program. If in doubt, consult your department head.

2. The departmental social media forum should indicate that it is not the official departmental source for information and a link to the department or county web site should be included where possible.
3. As with other county communication channels, social media communication should be professional, accurate, factual, timely, credible, and should promote the department's mission.
4. When information communicated in social media is in error, the responsible department must correct it as soon as possible.
5. When social media is used to allow public interaction or responses to employee-provided communication, an increased level of monitoring must be undertaken to ensure that the public responses are relevant to the topic and do not violate the Acceptable Use Policy for the Public. The department head or the designated employee assumes responsibility for monitoring the interaction or responses received from the public.
6. When a public response in a department's social media forum violates the Acceptable Use Policy for the Public or is determined to be off-topic, the authorized employee should record and then remove the response. How the response is recorded is determined by the department head. Where possible, the Acceptable Use Policy for the Public should be included in all social media forums where public interaction is enabled.
7. Department heads are responsible for the consistency, accuracy, and policy conformance of the content provided to social media on behalf of the department. Department heads may revise or remove content as needed.
8. The eGovernment Community of Interest (eGov COI) may periodically monitor department-related social media and may make suggestions to departments based upon best practices or analyses. In addition, the eGov COI serves as a resource for department staff members who wish to learn more about social media use at the County.

F. Security

1. This policy is not intended to supersede the County Information Security Policies (see "Policies" under [Information Security Program](#)). If inconsistencies or conflicts between the policies are found, the County Information Security Policies must be followed.
2. The security threats present in social media are similar to those in other web platforms. However, due to the widespread and instantaneous nature of social media, the harm caused by a realized threat can spread quickly. County employees must be aware of the following threats of particular concern to social media:
 - a. Phishing. Sometimes called spear phishing, a phishing attack in social media presents itself as a document, file, or a link that appears to be legitimate but is really an attack. The user is duped into viewing the

document or file or clicking the link. The opened document or linked web site may display information that appears to be valid, but in reality the attack has taken place--perhaps without being noticed until it's too late.

- b. Social Engineering. Due to the amount of users' personal information available on many social media sites, it is relatively easy to gather personal details about a particular individual. Social engineering is the threat that this information will be used by someone to pretend to be a county employee and perform a malicious act.
- c. Application Threats. Like other software, the applications with which social media sites function are subject to attack. When a familiar social media site begins to function in unexpected ways, an attack should be suspected. For example, when a site asks for the log in account to be entered in a new browser window or the site appears familiar but the browser displays an unfamiliar web address, a computer attack could be underway.

Social media sites are also a hub of third-party developed applications published by individuals or companies other than the social media provider. These applications often do not incorporate security and in the worst case they are designed to attack the user's computing device. To reduce the risk to the county network, employees must not download or install third party applications found on social media sites onto county computing assets.

- 3. In order to protect county computing assets, unnecessary functionality on social media sites such as instant messaging, file exchanges, and file uploads must not be used. Similarly, web links provided by the public will be prevented or eliminated to minimize the risk to the public of exposure to inappropriate or unauthorized material and security compromises. At the discretion of the department head, specific file interaction or linking on the part of the public may be allowed, but this requires additional rigor on the part of the responsible employees to monitor the sites for security compromises, such as image files with viruses or links that are phishing attacks.
- 4. County computing assets used to access social media sites must have up-to-date security patches and anti-virus or similar software installed. If a virus or other compromise is suspected, existing policies must be followed. Please see the Incident Response Policy in the [Information Security Program](#) (under "Policies").

G. Public Records Retention

Information communicated in social media must be retained by the department in compliance with the law and/or the County or department's record retention schedule. If in doubt about whether information needs to be retained or the length of retention, please check with your department head before deleting any social media content. To facilitate compliance, the department must use the social media

service's email updates feature when it's available. This feature automates update notification to employees when new entries are posted by the public.

The *Acceptable Use Policy for the Public* stipulates that any interaction or responses on the part of the public becomes public information and may also be subject to the Public Records Act. This policy should be made available to the public on all social media forums where possible.

IV. RESOURCES

- A. [List of County Standards Committee approved social media.](#)
- B. [Social Media Approval Form.](#)
- C. [Acceptable Use Policy for the Public.](#)
- D. [Information Security Program Policies.](#)
- E. [Human Resources Policies.](#)
- F. [County's Mission, Vision, and Organizational Values.](#)
- G. [The Brown Act.](#)
- H. [California Public Records Act.](#)
- I. Microsoft Safety and Security Center [password checker.](#)

V. OTHER AGENCY INVOLVEMENT

Agency	Action
County Counsel	Reviewed.
eGovernment Executive Steering Committee	Reviewed.
IT County Standards Committee	Reviewed.

BOS Approval Date: March 6, 2012

Effective Date: April 1, 2012