

Social Media Guidelines: King County#

1. PURPOSE

The role of technology in the 21st century workplace is constantly expanding and now includes social media communication tools that facilitate interactive information sharing and collaboration. Many of these websites and tools have large, loyal user bases and are, thus, increasingly important outreach and communication tools for government entities from the federal to the local level.

Social networking can improve interactivity between government agencies and the public, and often reaches new and different populations from traditional media.

King County agencies should have communication plans that include social media strategies. In doing so, however, county agencies should take care to choose a combination of traditional methods and social media that provide tools that distribute information across multiple outlets to the broadest audience.

All agency communication tools should be used in ways that provide clear communication, maximize transparency, maintain the security of the county network, and are appropriately professional. Social media is no exception. Therefore, the application of social media within King County agencies must be done thoughtfully and in a manner that will minimize risk. Social media users should be aware that these types of communications are considered public records and must be kept for a certain period of time in compliance with the public records law.

These guidelines are intended to ensure that agency-sponsored social networking sites are secure, appropriately used, and managed through best practices for the use of social media in King County government. This policy is designed to protect employees and ensure consistency across agencies when incorporating social media into their mission.

2. DEFINITIONS

- 2.1 Social Media: describes the online technologies, tools and practices that people use to share opinions, insights, experiences, and perspectives. Social media can take many different forms, including text, images, audio, and video. These sites typically use technologies such as webistes, blogs, message boards, podcasts, wikis, and video logs to allow users to interact.
- 2.2 Web Master and Web Team: Central Information Technology and Communications staff responsible for the overall direction of kingcounty.gov and enterprise web pages.
- 2.3 Chief Information Officer (CIO): Executive Branch Senior Technology Manager.
- 2.4 Communications Director: Director of Communications Director for the King County Executive.
- 2.5 Authorized Agent: King County employee who been authorized by their elected official, or department head or the County Communications Director to post content on behalf of their County agency social media websites.

- 2.6 County agency means:
- a) The executive branch;
 - b) The legislative branch;
 - c) The superior court;
 - d) The district court;
 - e) The department of public safety;
 - f) The department of assessments;
 - g) The office of the prosecuting attorney;
 - h) The department of elections;
 - i) The forecast council and office of economic and financial analysis;
 - j) The board of appeals; and
 - k) The personnel board.

3. APPLICABILITY

These guidelines are applicable to county employees or contractors who create or contribute to social networks, blogs, wikis, or any other kind of social media both on and off the www.kingcounty.gov domain for work purposes.

4. IMPLEMENTATION

Every agency needs an adopted communications plan with a clear strategy for how social media fits into this strategy. The Director of Communications for each agency should spearhead this activity and, in doing so, should consider the following questions when determining whether use of social media is appropriate:

- Who is the target audience for social media communications?
- What information is the agency/department attempting to communicate? Which social media tools are the best to distribute this information?
- Who is responsible for managing the different social media tools/accounts? Will this person represent the agency appropriately? Has staff been properly trained in the use of social media? What team of people will back the primary user in the event of vacation, emergency or job transitions? If a consultant's work includes social media outreach, which accounts will be used and who will approve content?
- What are the agency's responsibilities regarding collection and records retention including preservation of social media content? What does the records retention schedule require for these records?

When an agency/department decides to use a form of social media that is deemed beneficial to its mission, it should first establish protocols for using the service. It is important for agency/managers to communicate expectations of appropriate usage for social media within the workplace.

There should be an authorization process for employees wishing to create an account for the benefit of the agency, with the agency/department Director of Communications (or designee) as the authority to oversee and confirm decisions. In this role, the Director of Communications will evaluate all requests for usage, verify staff

Social Media Guidelines: King County#

3

being authorized to use social media tools, and confirm completion of online training for social media. The agency/department Director of Communications will work with communications staff in the King County Executive's Office and shall supply staff in KC IT with applicable passwords per the social media Executive Branch policy.

The agency Director of Communications (or his/her designee) will also be responsible for supplying a list of all social networking application names in use, the names of all employee administrators of these accounts, as well as, the associated user identifications and passwords currently active within their respective agencies to the KCIT Web Team. Should the employee who administers the account be removed as administrator or no longer be employed by the agency, the Department Director of Communications should immediately change all passwords and account information to maintain agency control.

Any agency-related social networking usage implemented prior to the release of this document should be reviewed by the Director of Communications to make sure it is brought into compliance with these guidelines.

In summary, the Director of Communications will:

- Oversee and confirm decisions regarding social media sites including authorization of sites
- Evaluate requests for usage
- Have final authority to edit or remove content within legal constraints per the PRC policy
- Verify staff being authorized to use social media tools
- Maintain a list of social media domains, active account logins and passwords
- Change passwords if employee is removed as administrator in order to maintain agency control
- Ensure social media material is archived including providing a list of all social media urls and contact information

4. ACCEPTABLE USE

All use of social networking sites by county agencies/departments should be consistent with applicable state, federal, and local laws, regulations, and policies including all information technology security policies. This includes: First Amendment rights; acceptable use policies; applicable records retention schedules or policies; procedures, standards, or guidelines used by the Executive Office, Prosecuting Attorney's Office, and OIRM. All usage should be governed by these policies as well as this policy and the one adopted by the PRC.

Personal responsibility:

Be thoughtful about how you present yourself in online social networks, where the lines between public and private, personal and professional are blurred.

Wherever possible, consider the following issues:

- **Confidentiality**- Employees will not post or release proprietary, confidential, sensitive or personally identifiable information or county government intellectual property on social media websites.

Social Media Guidelines: King County#

4

- **De minimis use-** Employees must adhere to the county de minimis use policy governing de minimis use. If you are not certain about the criteria for de minimis use, consult your agency policies or ask an agency supervisor or human resource consultant.
- **Disclaimers-** If employees identify themselves as a county employee on a social networking site, wherever appropriate, use a disclaimer (e.g. “While I work for King County, anything I publish is my personal opinion and not necessarily the opinions or position of King County government.”)
- **Personal vs. professional use-** Employees’ personal social-networking sites should remain personal in nature and should not be used for work-related purposes. Employees should not use their county e-mail account or password in conjunction with a personal social networking account.
- **Ethical obligations-** Some county ethical obligations must be followed at all times, even when employees engage in social media use in their personal capacities. For example, employees must not disclose confidential information acquired by the employee by reason of the employee’s official position. This restriction applies regardless of whether the information is disclosed on a personal or a county social media site.

Personal Use

Employees are allowed to have personal social networking sites. Employees should never use their county email account or password in conjunction with a personal social networking site. During normal business hours, employees may use personal social networking for limited family or personal communications so long as those communications do not interfere with their work and as long as they adhere to existing computer use policies. Should employees discuss their county work on personal social networking accounts or web sites, they should be aware their account may be subject to public disclosure laws, even if produced on personal time and equipment.

Professional Use:

All agency-related communication through social media outlets should remain professional in nature and should always be conducted in accordance with the agency’s communications policy, practices, and expectations. Employees must not use social networking sites for political purposes, to conduct private commercial transactions, or to engage in private business activities. Employees should be mindful that inappropriate usage of social media can be grounds for disciplinary action. If an account is used for business, the entire account, regardless of any personal views, is subject to this policy, including the collection and preservation provisions.

Identity yourself clearly:

When creating social media accounts that require individual identification, county employees should use their actual name, not pseudonyms. However, using actual names can come with some risks. Any employee using his or her name as part of a county agency’s application of social media should be mindful of the following:

- Do not assume privacy. Only post information that you are comfortable disclosing.
- Use different passwords for different accounts (both social media and existing work accounts). Using the same password for all accounts increases the vulnerability of the accounts being compromised.

Ethics:

Employees should be mindful of the King County [Employee Code of Ethics](#). The Code of Ethics applies to social media content and use.

Terms of Service:

Employees should be aware of the Terms of Service (TOS) of the particular form of media. Each form of social media has its own unique TOS that regulate how users interact using that particular form of media. Any employee using a form of social media on behalf of a county agency should consult the most current TOS in order to avoid violations. If the TOS contradict agency policy then the PIO should be made aware and a decision should be made about whether use of such media is appropriate.

5. CONTENT MANAGEMENT

Clear comment policies for users:

Whenever possible, county social media web sites should clearly outline Terms of Use and Comment policies.

Content of Posts and Comments:

Employees using social media to communicate on behalf of a county agency should be mindful that any statements made are on behalf of county government; therefore, employees should use discretion before posting or commenting. Once these comments or posts are made, they can be seen by anyone and usually cannot be deleted. Consequently, communication should include no form of profanity, obscenity, or copyright violations. Likewise, confidential or non-public information should not be shared. Employees should always consider whether it is appropriate to post an opinion, commit oneself or one's agency to a course of action, or discuss areas outside of one's expertise. If there is any question or hesitation regarding the content of a potential comment or post, it is better not to post. There should be great care given to screening any communication made on behalf of the agency using this social media as improper posting and use of social media tools can result in disciplinary action. It is also not appropriate to engage in arguments with members of the public who may be critical of your agency.

6. RECORDS RETENTION

Communication through agency-related social media is considered a public record and will be managed as such. All comments or posts made to County agency account walls or pages are public, not private. This means that both the posts of the employee administrator and any feedback by other employees or non-employees, including citizens, will become part of the public record. Because others might not be aware of the public records law, agencies should include the following statement (or some version of it) somewhere on the social networking Web site:

Representatives of King County government communicate via this Web site. Consequently any communication via this site (whether by a county employee or the general public) may be subject to monitoring and disclosure to third parties.

In the spirit of transparency, account administrators who receive messages through the private message service offered by the social media site should encourage users to contact them at a public e-mail address maintained by their agency. For private messages that account administrators do receive, they should be treated as constituent e-mails and therefore, as public records. Account administrators or another authorized staff member should reply using their county e-mail account.

Social Media Guidelines: King County#

6

Agencies should set all privacy settings to public.

Agencies must assume responsibility for public records and adhere to the schedule set by the Washington State Archives.

7. SECURITY

Agencies should consider how to prevent fraud or unauthorized access to social media sites. In almost every case where an attacker accesses a system without authorization, he/she does so with the intent to cause harm, including:

- Making unofficial posts, tweets or messages that will be seen by the public as official messages.
- Encouraging users to either click links or download unwanted applications that the attacker has added to the site.
- Accessing, compromising or disabling a county system.
- Redirecting users to sites that look like a state site but are used to gather data that could be used for unauthorized purposes (i.e. phishing).
- Using a compromised site to spread malware.
- Acquiring confidential information about state employees or citizens (i.e. social engineering).

Use best practices to mitigate security risks

Security related to social media is fundamentally a behavioral issue, not typically a technology issue. In general, employees unwittingly providing information to third parties pose a risk to the state network. Employees need to be aware of current and emerging threats that they may face using social media website and how to avoid falling prey. If agencies participate in social networking, agencies should:

- Use a separate user IDs and password to access social networking sites.
- Never duplicate user IDs and passwords across multiple social networking sites.
- Never use your King County network login and password for a social media web site
- Train users about what information to share, with whom they can share it, and what not to share.
- Educate users about security awareness and risks when using social media.
- Help employees set appropriate privacy settings for social networking websites.
- Update current Acceptable Use Policies to cover user behavior for new media technologies. User behavior includes personal use of government equipment, de minimis use, and professional use of internal facing, public facing, and external resources.
- Consider disaster recovery requirements in the event that your agency hosts your own social media services. Work with your agency's IT department to establish clear recovery time objectives.
- Regularly apply Microsoft patches.
- Review (and apply as appropriate) patches for Firefox, Adobe and Java as these softwares are common paths for security vulnerabilities.

8. TOOLS AND SOFTWARE

Social media tools and trends change rapidly and King County Information technology will work to keep up with recent trends. All new social media tools will be approved by the King County CIO and the Executive's Director of Communications.

- The OIRM Web Team will maintain a list of currently supported social media web sites and tools
- The OIRM Web Team will provide training materials and workshops on currently supported tools
- The OIRM Web Team will offer advice on measuring effectiveness of social media tools
- Agencies are responsible for maintaining their own public records surrounding social media
- Branding standards will be established by the Executive's Director of Communications

9. REFERENCES

Special thanks to Washington State Governors office for their Social Media Guidelines from which much of this document was modeled.

Federal & Private Entities

- [CIO Council's Guidelines for Secure Use of Social Media by Federal Departments and Agencies](#)
- [General Services Administration Social Media Handbook](#)
- [General Services Administration Social Media Policy](#)
- [IBM Social Computing Guidelines](#)

City, State and Local

- [Best Practices for Social Media Usage in North Carolina](#)
- [City of Seattle Social Media Use Policy](#)
- [City of Seattle City Council](#)
- [Massachusetts Governor's Office Social Media Usage and Policies](#)
- [New York State Social Media Policy](#)
- [State of Oregon Social Networking Guide](#)
- [State of Utah Social Media Guidelines](#)
- [Washington State Attorney General's Office Blog Comment and Use Policy](#)
- [Washington State Department of Ecology Blog Commenting Policy](#)
- [Washington State Department of Licensing Blog Use Policy](#)
- [Washington State Department of Information Services Posting to Social Networking Sites](#)
- [Washington State Department of Transportation Comment Policy](#)
- [Washington State Labor and Industries Social Media Policy](#)
- [Washington State Secretary of State Blog Use Policy](#)
- [Washington State Secretary of State Blogs, Wikis, Facebook, Twitter & Managing Public Records](#)