

1317

1-7

10/21/14

1.0 PURPOSE:

To establish City of West Allis (City) general standards and responsibilities for the acceptable use of Social Media.

2.0 ORGANIZATIONS AND PERSONS AFFECTED:

This policy applies to all City of West Allis officers, departments, boards, commissions, volunteers and employees [except protective service employees, unless otherwise included by City Ordinance or Policy and Procedure]. This policy also applies to users who comment or otherwise interact with the City through its Social Media websites.

3.0 POLICY:

The role of technology in the 21st century workplace is constantly expanding. Social Media tools such as Facebook, Twitter and blogs can improve interactivity between government and the public, reaching new and different populations from traditional media sources. City of West Allis Departments should choose a combination of traditional media and Social Media sources that complement each other and distribute information to relevant audiences. This Policy governs the use, administration, management, monitoring, and retention of Social Media and Social Media Content, consistent with state, federal and local laws and regulations, and City and Departmental goals.

4.0 REFERENCES:

City of West Allis Electronic Communication Policy 1311
 Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510 - 2711)
 Wisconsin Statutes Section 947.0125
 Wisconsin Social Media Protections Act (Wisconsin Statutes Section 995.55)

5.0 DEFINITIONS:

- Authorized Social Media User or Authorized User – Any City Officer or employee responsible for the use, administration, management, monitoring, and/or retention of Social Media, Social Media tools or web sites, and/or Social Media Content, in the name of or on behalf of the City or any City agency.
- Blog – A blog (short for web-log) is an online journal, irrespective of length, that is frequently updated and intended for general public consumption. Blogs generally represent the personality and opinion of the author or reflect the purpose and opinion of the website that hosts the blogs.

- City Social Media Accounts – Any blog, chat room, forum, social networking site and/or website under the direction and control of the City of West Allis, including, but not limited to, all City Officers, Departments, Boards, Committees, Commissions, or Authorities.
- City Officer – Any City of West Allis elected or appointed Official or any member of a City Board, Commission, Committee, or Authority.
- Covered Personnel – Any City Officer or employee.
- Forum – An online discussion group where users can post comments and thoughts, either anonymously or with personal identity.
- Limited Public Forum – A public forum created by the government voluntarily for expressive activity that may be restricted as to subject matter or class of speaker.
- Personal Social Media Accounts – Any blog, chat room, forum, social networking site and/or website created or configured by an individual for individual, social, or entertainment purposes. (Examples include, but are not limited to, Facebook, Foursquare, Twitter, and Google+).
- Posts – A comment or thought left by a user on a blog, social media site, or as in the comment pages of news articles found on the like of JSOnline.com or the WestAllisNow web sites.
- Site Administrator – A designated City employee responsible for administering a City Social Media Account.
- Social Media – Internet technologies that facilitate and promote interactive communication, participation, and collaboration. Examples of social media include, but are not limited to, the web sites and applications Blogger, Facebook, LinkedIn, Twitter, Tumblr, Foursquare, Meetup.com, Flickr, YouTube, Yelp, Second Life, and Wikipedia, and the interactive tools and functions they provide to users.
- Social Media Content – Any materials, documents, photographs, graphics, and other information that is created, posted, distributed, or transmitted using Social Media Internet sites or Social Media tools.

6.0 PROCEDURES:

All City Social Media Accounts shall be operated in conformance with, and be consistent with applicable state, federal, and local laws, regulations and policies, including all information technology security policies, public record laws and applicable record retention laws. Covered Personnel shall not blur or combine their personal and professional lives when operating City or Personal Social Media Accounts. **The guidelines and restrictions within this Policy should not be construed in a manner that unlawfully interferes with any applicable employee rights provided under state or federal law, including but not limited to, Section 7 of the National Labor Relations Act.**

6.1 Department Heads and City Officers

- 6.1.1 Departments shall only establish, use or terminate a Social Media identity, account, profile, page, or site (collectively, City Social Media Account(s)) with the approval of the Department Head and Director of Information Technology and Communications or his/her designee. City Officers shall consult with the Director of Information Technology and Communications or his/her designee prior to establishing, using, or terminating a Social Media Account. The establishment and maintenance of any City Social Media

Account shall be done in accordance with the procedures implemented by the Director of Information Technology and Communications.

- 6.1.2 Department Heads may designate one or more employees to be Authorized Social Media User(s) for the Department. Only the Department's Authorized Social Media User(s) shall be authorized to post Social Media Content on the Department's City Social Media Accounts and may have access to the Department's City Social Media Accounts that permit such posting.
- 6.1.3 Department Heads whose Departments have Social Media Accounts shall establish guidelines for all Social Media Content that is posted on the Department's City Social Media Accounts, including the designation of one or more Department managers (who may also be Authorized Social Media Users) to be responsible for approving content if needed. All Department-established Social Media guidelines and policies must be consistent with this Policy and any guidelines and procedures established by the Director of Information Technology and Communications, and must be approved by the Director of Information Technology and Communications or his/her designee. City Officers shall comply with the guidelines and procedures established by the Director of Information Technology and Communications for posting on City Social Media Accounts.
- 6.1.4 No Authorized User's information or link (hyperlink) to any Internet site or other materials or communications may be posted, or approved for posting, on a City Social Media Account that is not directly related to the mission, services, goals and objectives of the City, or a Department, Board, Commission, Committee or Authority of the City.
- 6.1.5 City Social Media pages must clearly identify the pages as created and managed by the applicable Department, Office, Board, Commission, Committee or Authority of the City.
- 6.1.6 All City Social Media Accounts must prominently display, on the first page accessible to site visitors, links to the City's official Internet site www.westalliswi.gov.

6.2 Authorized Social Media Users

- 6.2.1 No Authorized Social Media User may establish any City Social Media Account in the name of or on behalf of the City or any City Department that has not been approved by the Department Head and the Director of Information Technology and Communications or his/her designee.
- 6.2.2 Authorized Users shall use City Social Media Accounts for City and Department business purposes only. Use for communications and postings that are not directly related to a City or Department business purpose is prohibited.
- 6.2.3 City Social Media Accounts must be monitored regularly and content kept current with updates and/or new postings. City Social Media Accounts are not meant to replace the City website for official dissemination of City information. Information found on City Social Media Accounts may also be placed, as deemed appropriate, on the City website.
- 6.2.4 Authorized Social Media Users must report unauthorized uses of City Social Media or City Social Media Accounts to their Supervisor, Department Head, and/or the Director of Information Technology and Communications or his/her designee, as applicable.

- 6.2.5 Authorized Social Media Users are expected to be attentive and careful in their use of Social Media. Authorized Social Media Users should be aware that their personal use of Social Media may be perceived as representing the City and City government, and should tailor their use accordingly.
- 6.2.6 When a City of West Allis Authorized Social Media User responds to a comment, in his/her capacity as a City of West Allis representative, their name and title shall be included.
- 6.2.7 City Social Media Accounts should not connect with ('friend' or 'like') or follow private entities or individuals but may connect with ('friend' or 'like') or follow other organizations who share similar missions.
- 6.2.8 Authorized Social Media Users who receive messages through the private message service offered by some Social Media must have users contact them at their City supplied email address. Any such messages received will be treated as work-related emails and therefore, as public records.

6.3 Public Users

- 6.3.1 City Social Media Accounts or pages may be "limited public forums" under the First Amendment if visitors post comments or other communications.
- 6.3.2 If interactive communications (e.g. comments) are permitted on City Social Media Accounts, the terms of use for visitors to the site will be posted prominently on the site, unless prohibited by the terms of use governing the specific City Social Media Account or prevented by the site.
- 6.3.3 Every City Social Media Account will have a clear description of the topics the account is intended to address and that may be addressed in comments. User postings will be removed if they are not directly related to those topics or are determined to be unacceptable use.
- 6.3.4 Visitors to the City Social Media Accounts must comply with the terms of use and privacy policies of the site operator, and are subject to the site operator's practices regarding the collection and retention of passive information (e.g. cookies) and other information from and about visitors.
- 6.3.5 All postings by visitors to City Social Media Accounts will be retained by the City, as required by applicable law, City Policy and/or procedure established by the Director of Information Technology and Communications.
- 6.3.6 All postings may be subject to public records and disclosure laws, as well as discovery in litigation. This includes, but is not limited to, information made available through a user's privacy settings on their own Social Media and other Internet pages.
- 6.3.7 Visitors to the site should have no expectation of privacy or confidentiality with respect to any content they post to the site, and the City has no responsibility for maintaining any such privacy or confidentiality.
- 6.3.8 A comment posted by a member of the public on any City Social Media Account is the opinion of the commentator or poster only, and publication of a comment does not imply endorsement of, or agreement by, the City, nor do such comments necessarily reflect the opinions or policies of the City.

6.3.9 The City reserves the right to deny access to City Social Media Accounts to any individual who violates this Social Media Policy, at any time and without prior notice.

6.3.10 Communications that are unacceptable uses, as identified in Section 6.5 below, will be removed and documented.

6.4 Personal Social Media Accounts

6.4.1 Using Non-City Information Systems: This Policy is not intended to govern Covered Personnel's establishment or use of Personal Social Media Accounts for personal purposes, on non-work time, and using non-City information systems. However, because some such personal uses of Social Media may reflect on the City by appearing to represent City Policy and/or views or to be on behalf of the City, the following criteria apply to Covered Personnel's use of Personal Social Media Accounts, regardless of whether they use City or non-City information systems:

6.4.1.1 These sites must remain personal in nature and be used to share personal opinions or information. Postings and user profiles on Personal Social Media Accounts must not state or imply that the views, conclusions, statements or other Social Media content are an official policy, statement, position, or communication of the City of West Allis, or represent the views of the City or any City Officer or employee acting in their official capacity.

6.4.1.2 Covered Personnel should never use their City email accounts or passwords in conjunction with their Personal Social Media Accounts (e.g., they must access these sites through their own personal email accounts such as Gmail, yahoo, etc.).

6.4.1.3 Covered Personnel are not allowed to access their Personal Social Media Sites on work time.

6.4.1.4 Covered Personnel must not conduct any official City business on their Personal Social Media Accounts.

6.4.2 Using City Information Systems: In addition to the criteria set forth in 6.4.1.1 – 6.4.1.4 above, Covered Personnel accessing and using Personal Social Media Accounts by means of City information systems are subject to the following criteria:

6.4.2.1 Covered Personnel shall comply with all applicable City Policies and Rules (e.g., Electronic Communications Policy 1311).

6.4.2.2 Covered Personnel have no right to, nor should they expect or assume privacy or confidentiality with respect to their personal use of Social Media or Personal Social Media Accounts accessed by means of City information systems, or with respect to personal Social Media content so accessed. By utilizing the City's information systems to access and use their Personal Social Media Accounts, Covered Personnel acknowledge that the City is free to view, monitor and record all activities at any time without consent or prior approval (see Section 5.4 of the City's Electronic Communication Policy 1311).

6.5 Unacceptable Uses

The City considers the activities and uses of Social Media listed below to be unacceptable. City Officers, employees and public users are prohibited from engaging in any of these unacceptable uses on a City Social Media Account:

- 6.5.1 Using Social Media in a manner that does not comply with federal, state, and local laws and regulations or with City and Department policies.
- 6.5.2 Using Social Media in a manner that:
 - 6.5.2.1 Violates the copyright, trademark, or other intellectual property rights of any person or entity, or otherwise violates their legal ownership interests;
 - 6.5.2.2 Includes ethnic slurs, profanity, personal insults; includes material that is harassing, defamatory, fraudulent or discriminatory; and/or includes other content or communications that would not be acceptable in a City workplace under City or Department Policy or Practice;
 - 6.5.2.3 Violates the terms of contracts governing the use of any Social Media Content, including but not limited to, software and other intellectual property licenses;
 - 6.5.2.4 Displays sexually explicit images, cartoons, jokes, messages, or other material in violation of the City's Anti-Harassment and Retaliation Policy 1436;
 - 6.5.2.5 Violates City Policy and/or Rules and Regulations relating to "Political Activities" (e.g., Policy 1423; Rule IX, Section 1 s) of the Civil Service Commission Rules and Regulations, etc.;
 - 6.5.2.6 Contains confidential or "for official use only" information or information that compromises the security of City networks or information systems. Such "confidential" or "for official use only" information includes, but is not limited to, information that is protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or other federal, state, or local laws and regulations (except as permitted under such laws and regulations), as well as social security numbers and other personally identifiable information. "Confidential information" does not include terms and conditions of employment;
 - 6.5.2.7 Violates the terms of use governing the City Social Media Account.

This list is not exhaustive. Questions about particular uses of Social Media or particular Social Media Content should be directed to the Department Head and/or the Director of Information Technology and Communications or his/her designee who, in turn, shall consult with the City Attorney as necessary.

6.6 Security

- 6.6.1. From a security standpoint, Authorized Users should be mindful of how to best prevent fraud or unauthorized access to the City Social Media Accounts. In almost every case where an attacker accesses a system without authorization, they do so with the intent to cause harm.

- 6.6.2. In order to minimize the possibility of security or confidentiality breaches of City Social Media Accounts, Authorized Users must:
 - 6.6.2.1 Be aware of which information to share, with whom they can share it, and what not to share;
 - 6.6.2.2 Participate in Social Media security training designed to educate Authorized Users about the risks of information disclosure when using Social Media, and make them aware of various attack mechanisms;
 - 6.6.2.3. Be aware of Privacy Act requirements and restrictions. Read each Social Media site's terms of service, usage policies and privacy controls to help protect their own privacy in any profile they use for work-related activities and more effectively protect against inadvertent disclosure of sensitive City information; and
 - 6.6.2.4. Comply with the City's Code of Ethics and any other applicable City Policies and Regulations governing their behavior.
- 6.6.3. Passwords –To prevent unauthorized users access to City Social Media Accounts, each Authorized Social Media User shall follow City Policies (e.g., Electronic Communication Policy 1311) and any procedures established by the Director of Information Technology and Communications, that address passwords.

7.0 RECORDS MANAGEMENT AND RETENTION:

Communication through City Social Media Accounts is considered a public record. All City Social Media Accounts shall adhere to applicable state, federal and local laws, regulations and policies, including all Information Technology and Records Management Policies of the City, as well as other applicable City policies. The Wisconsin Public Records Law applies to Social Media Content and therefore, such content within City Social Media Accounts must be able to be managed, stored and retrieved to comply with these laws. Department Heads and designated City Officers will be responsible for any public records within their City Social Media Accounts and compliance with the applicable record management laws and policies of the City.

All content created, received, transmitted, stored on, or deleted from City information systems is exclusively the property of the City or, to the extent provided by applicable law, of the person or entity that created or owns the copyright or trademark rights to that content.

8.0 POLICY COMPLIANCE AND VIOLATION:

Department Heads shall be responsible for compliance and enforcement of this Policy within their Departments. The Director of Information Technology and Communications or his/her designee shall be responsible for compliance and enforcement of this Policy with respect to City Officers.

Covered Personnel who violate this Policy, or any other City or Department policy or procedure pertaining hereto, may be subject to disciplinary action, up to and including termination of employment.