



Social Media Policy

Updated Sept. 9, 2017

1.0 PURPOSE:

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

2.0 ORGANIZATIONS AND PERSONS AFFECTED:

This policy applies to all City Officers, departments, boards, commissions, committees, authorities, volunteers and employees [except protective service employees, unless otherwise included by City Ordinance or Policy and Procedure]. This policy also applies to public users who interact, publish, or post content to City Social Media.

3.0 POLICY:

Technology continues to expand and redefine interactions within communities. Social Media tools can improve interactivity and involvement between government and the public in ways that reach new and different populations beyond the scope of traditional media outlets. The City and its City Officers, departments, boards, commissions, committees, and authorities, may choose a combination of traditional media and social media to complement each other in order to disseminate information and engage the community. The City has a fundamental interest and obligation to manage and monitor information that is disseminated by and through Social Media Accounts associated with the City. This policy governs the use, administration, management, monitoring, and retention of Social Media and Social Media Content, consistent with state, federal, and local laws, regulations and in line with City goals.

4.0 REFERENCES:

City of West Allis Electronic Communication Policy 1311
City's Anti-Harassment and Anti-Retaliation Policy 1436
City's Political Activities Policy 1423
Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-2711)
Wisconsin Statutes Section 947.0125
Wisconsin Social Media Protections Act (Wisconsin Statutes § 995.55)

5.0 DEFINITIONS:

- Authorized Social Media User (hereinafter "Authorized User") - A City Officer or employee responsible for the creation, use, publishing, posting, 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 officers, departments, boards, commissions, committees and authorities, volunteers and employees.

- Blog- (short for web-log) 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.
- Candidate website- Means a website or social media account for a person currently running for a political office or position.
- City Officer- Any City elected or appointed official or any member of a City board, commission, committee, or authority.
- City Social Media Accounts- Any blog, chat room, forum, social media site and/or website under the direction and control of the City, including, but not limited to, all City Officers, departments, boards, committees, commissions, or authorities.
- City Information System- A system designed for the collection, organization, storage, and communication of information as run and controlled by the City.
- Cookies- An electronic packet of data sent by an internet server and a browser or website used to identify the user or track his/her access to the server.
- Corporate Commercial Website- means a promotional website or social media account for a corporate commercial entity.
- Covered Personnel- Any City Officer, employee, or volunteer.
- Forum- An online discussion group where people can post comments, information, images, or other electronic content, either anonymously or with personal identity.
- Interactive Communication- A dynamic flow of information where users or participants can engage in two-way communication rather than simply passive observation of information.
- 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.
- Link or Hyperlink- A hypertext file or document which connects a user to another location or file, typically activated by clicking on a highlighted word or image on the screen.
- Malware- Software that is intended to damage or disable computers and computer systems or electronic communication devices.
- Personal Identification Information- Information and documents as defined under Wisconsin Statute Sections 943.201(1)(a) and (b).
- Personal Social Media Accounts- Any blog, chat room, forum, social media site and/or website created or configured by an individual or entity for individual, social, or

entertainment purposes. (Examples include, but are not limited to, Facebook, Foursquare, Twitter, and Google+).

- Posts- Comments, information, images, or other electronic content left by a user/person on a blog, social media site, or other website.
- Public User- Any person or entity utilizing a personal social media account who is not acting as an Authorized User. Covered Personnel using a personal social media account may also be a public user if they are not acting in their capacity as an Authorized User.
- Publish- Comments, information, images, or other electronic content that is made or disseminated via social media, websites, or other publically open electronic forum.
- Site Operator- The entities that manage or control each social media platform (e.g. Facebook, Google, Instagram, LinkedIn, etc.)
- 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 messages, materials, documents, photographs, videos, graphics, and other information that is created, posted, distributed, transmitted, or published using Social Media internet sites or Social Media tools.
- Visitor- Any person or entity who is not acting in the name of or on behalf of the City or any City officers, departments, boards, commissions, committees and authorities, volunteers and employees, that uses, posts, views, or otherwise utilizes a City Social Media Account.
- Volunteer- A person recognized and authorized by the City to perform services for the City without promise, expectation, or receipt of compensation for services rendered. The receipt of reimbursement for authorized expenses does not constitute compensation as used herein.
- Work Shift- The assigned or designated period of time that the Authorized User engages in City employment-related activities for arranged or negotiated compensation.

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 Communications Department:

- 6.1.1 The Communications Department, by the Director of Communications or his/her designee, shall oversee City Social Media Accounts. This includes, but is not limited to:
- a. Developing standards and processes for creating and managing City Social Media accounts (i.e. operational and use guidelines).
 - b. Ensuring compliance of this policy and any guidelines developed thereunder.
 - c. Authorizing the creation of City Social Media Accounts.
 - d. Confirming the appointment of Authorized Users.
 - e. Maintaining accurate lists of City Social Media Account domains, log-in information, and passwords.
 - f. Ensuring that a City Social Media Account's password and/or log-in information is changed upon the designation of a different Authorized User to that account.
 - g. Developing departmental and city-wide branding/design standards
- 6.1.2 The Director of Communications or his/her designee shall be authorized to immediately edit or remove posts on City Social Media Accounts that violate this policy. Where practicable, Director of Communications or his/her designee will consult with the City Attorney's Office prior to deleting content.

6.2 Department Heads and City Officers:

- 6.2.1 Departments shall only establish or terminate a City Social Media Account with the approval of the department head AND the Director of Communications or his/her designee.
- 6.2.2 City Officers shall consult with the Director of Communications or his/her designee prior to establishing or terminating a City Social Media Account. The establishment and use of a City Social Media Account shall be done in accordance with the procedures implemented by the Director of Communications. City Officers with a City Social Media Account will be deemed to be the Authorized User for that City Social Media Account
- 6.2.3 The department heads of whose departments have City Social Media Accounts may designate one employee per shift to be an Authorized User for the Department. The department head may be the Authorized User. Only the department's Authorized User(s) shall post Social Media Content on the department's City Social Media Account(s). In the event that the department's Authorized User is unavailable, the department head may utilize the City Social Media Account or may contact the Communications Department to publish proposed content for the Department.

- 6.2.4 Department heads shall inform the Director of Communications or his/her designee of any changes to Authorized Users as soon as reasonably practical.
- 6.2.5 Department heads whose departments have City Social Media Accounts must comply with this policy. Those departments with City Social Media Accounts may also create additional guidelines for their accounts only if those guidelines are consistent with this Policy and are more restrictive than this policy, any guidelines established hereunder by the Director of Communications, and are approved by the Director of Communications or his/her designee. City Officers shall comply with this Policy for posting on City Social Media Accounts and may seek guidance or clarification from the Communications Department.
- 6.2.6 For each City Social Media Account that is approved for use, the Authorized User must provide the following documentation to the Communications Department:
- a. A signed and dated operational and use guidelines (The department shall adopt this Policy in its entirety and may create its own guidelines in addition to this Policy per 6.2.4. A signed copy of this policy, in addition to any other social media guidelines implemented by the department, must be provided to the Communications Department).
 - b. Signed and dated "Terms of Use" and the privacy controls/policy for each Social Media Account and each Authorized Social Media User. For example, if the department has a Facebook page, each authorized user will be required to print the general Facebook "Terms of Use," review said document, and sign and date that s/he has read the document.
- 6.2.7 City Social Media pages must clearly identify the pages as created and/or managed by the applicable department, board, officer, commission, committee, or authority of the City.
- 6.2.8 All City Social Media Accounts must prominently display, on the first page accessible to site visitors, hyperlinks to the City's official internet site at www.westalliswi.gov.

6.3 Authorized Users

- 6.3.1 No Authorized User may establish a City Social Media Account in the name of or on behalf of the City or any City Department unless the City Social Media Account has been approved by the Director of Communications, or his/her designee, and the department head of the department seeking to establish a City Social Media Account.

- 6.3.2 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 City or Department business purposes is prohibited.
- 6.3.3 Authorized Users are not permitted to share log-in information with anyone but the department head and/or the Director of Communications or his/her designee.
- 6.3.4 Any content that is published, posted, or hyperlinked to in any capacity by an Authorized User to a City Social Media Account must be related to a mission, service, goal, or objective of the City, department, officer, board, commission, committee, or authority of the City.
- 6.3.5 If possible via the Social Media platform, each City Social Media Account will have mission statement which will create a general topic for the City Social Media Account.
- 6.3.6 Any content published by the Authorized User must have a specific and declared topic to narrowly tailor discussions that may result from the published content. The Director of Communications or his/her designee may assist Authorized Users in creating and declaring discussion topics in order to help narrowly tailor discussions on City Social Media Accounts.
- 6.3.7 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 the City Social Media Accounts may also be placed, as deemed appropriate by the Director of Communications or his/her designee, on the City website.
- 6.3.8 Authorized Users shall report unauthorized uses of City Social Media Accounts to the Director of Communications or his/her designee as soon as the unauthorized use is discovered.
- 6.3.9 Authorized Users are expected to be attentive and careful in their use of City Social Media Accounts. Authorized Users shall not combine or mix Personal Social Media Accounts and activity with City Social Media Accounts. Authorized Users must be mindful that content posted on their Personal Social Media Account may be perceived as official City business and tailor their use of personal social media accordingly.
- 6.3.10 City Social Media Accounts shall not 'friend', 'like', 'follow', or otherwise connect with:
 - a. Candidate Sites or pages advocating a position on a City or other ballot issue. A city Social Media Account may remain connected

with a City Officer's City Social Media Account so long as the City Officer's City Social Media Account does not advocate a candidate or position on a City or other ballot issue.

- b. Corporate Commercial Websites that promote companies or subsidiaries whose business is derived from the sale or manufacture of tobacco products, alcoholic beverages, or sexual/adult-oriented products.
- c. Religious or political organizations.
- d. Individual Personal Social Media Accounts.

6.3.11 City Social Media Accounts may 'friend', 'like', 'follow', or otherwise connect with:

- a. Other City Social Media Accounts.
- b. Corporate Commercial Websites not prohibited by 6.3.10.b.
- c. Entities that have been identified by the City as being part of a City program promoting a neighborhood economic development for a target area.

6.3.12 If an Authorized User is communicating or messaging through an Authorized Social Media Account, the Authorized User must use a method of communication that is archived by the City and retained under records retention protocol. Any such messages received or sent will be treated as work-related emails and, as such, is open to public records.

6.3.13 Authorized Users may only use City Social Media Accounts during their normal working hours unless otherwise authorized by their department head. Overtime is not approved for Social Media usage outside of normal working hours unless prior approval has been granted by the User's department head.

6.4 Public Users

6.4.1 City Social Media Accounts will be considered "limited public forums" under the First Amendment on accounts that allow visitors to post comments, publish content, or otherwise allow public electronic communication.

6.4.2 If interactive communications are permitted on City Social Media Accounts, the terms of use for visitors to the social media page will be posted prominently on the City Social Media Account page, unless prohibited by the terms of use governing the social media account and the site operator.

6.4.3 Each discussion or thread with interactive communication capabilities must have a specific and declared topic or description of the topic which may be addressed by users in the comments or discussion section. Posts may be removed if they are not directly related to those topics or are determined to be an unacceptable use. See section 6.6 of this policy.

- 6.4.4 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.
- 6.4.5 All postings or publications on City Social Media Accounts will be retained by the City, regardless whether the content is posted by a Visitor, Public user, or Authorized User, as required by applicable law, City Policy and/or procedure established by the Director of Communications.
- 6.4.6 All postings may be subject to public records and disclosure laws, as well as discovery in litigation.
- 6.4.7 Visitors to the City Social Media Account page should have no expectation of privacy or confidentiality with respect to any content they post or publish to the site, and the City has no responsibility for maintaining any such privacy or confidentiality.
- 6.4.8 A comment posted or information published by a member of the public on any City Social Media Account is the opinion of the commenter or poster only, and publication of a comment does not imply any endorsement or agreement by the City, nor do such comments necessarily reflect the opinions or policies of the City.
- 6.4.9 Communications or publications that are unacceptable uses, as defined in Section 6.7 of this policy, may be removed by an Authorized User or Communications Department and documented by the department that removed the post.
 - 6.4.9.1 The procedure for documenting the unacceptable use will be determined by the Director of Communications or his designee but shall at least include retention of an electronic copy or physical copy of the unacceptable use including identification of the City Social Media Account affected and who had posted or published the unacceptable use.

6.5 Denying Access to City Social Media Accounts

- 6.5.1 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. A person who is denied access, banned, or otherwise blocked from a City Social Media Account will remain blocked for one (1) year and can submit a request through the specific City Social Media Account to be permitted access to that City Social Media Account after the one (1) year ban has expired.

- 6.5.2 Any person who is blocked by the City from a City Social Media Account may appeal that designation by submitting an appeal in writing to the City Clerk's Office. That appeal must occur during the one (1) year ban.

6.6 Personal Social Media Accounts

6.6.1 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:

6.6.1.1 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 or represent the views of the City or any City departments, officer, boards, commissions, committees, and authorities or Covered Personnel acting in their official capacity.

6.6.1.2 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.).

6.6.1.3 Covered Personnel must comply with Section 5.3 of the City's Electronic Communication Policy 1311 regarding use of access to Personal Social Media Sites on work time.

6.6.1.4 Covered Personnel must not conduct any official City business on their Personal Social Media Accounts unless required by the terms of use of the Social Media platform and authorized by the Director of Communications or his/her designee.

6.6.2 Using City Information Systems: In addition to the criteria set forth in 6.5.1.1-6.5.1.4 above, Covered Personnel accessing and using Personal Social Media Accounts by means of City Information Systems are subject to the following criteria:

6.6.2.1 Covered Personnel shall comply with all applicable City policies (e.g. Electronic Communications Policy 1311).

6.7 Unacceptable Uses

The City considers the activities and uses of Social Media listed below to be unacceptable. The City reserves the right to restrict or remove any content that is deemed in violation of this Social Media Policy or any applicable laws. Covered Personnel and Public Users are prohibited from engaging in any of these unacceptable uses on City Social Media Accounts:

- 6.7.1 Using City Social Media Accounts in a manner that does not comply with federal, state, or local laws and regulations, with City and department policies, or encourages illegal activity.
- 6.7.2 Using City Social Media in a manner that:
 - 6.7.2.1 Is not topically related to the particular City Social Media Account's mission statement or that has deviated off topic from the individual post or publication on the City Social Media Account;
 - 6.7.2.2 Violates the copyright, trademark, or other intellectual property rights of any person or entity, or otherwise violates their legal ownership interests;
 - 6.7.2.3 Includes content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status in regards to public assistance, national origin, mental or physical disability, or sexual orientation, or any other legally protected status;
 - 6.7.2.4 Contains language or content that is threatening, abusive, profane, or otherwise disorderly;
 - 6.7.2.5 Includes materials that is harassing or contains threats defamatory, fraudulent, or discriminatory content; and/or the post contains a violation of federal or state laws, local ordinances, or regulations;
 - 6.7.2.6 Violates the terms of use governing the use of any Social Media Content, including but not limited to software and other intellectual property license;
 - 6.7.2.7 Displays or hyperlinks to sexual content including but not limited to sexually explicit images, cartoons, jokes, messages, or other material in violation of the City's Anti-Harassment and Anti-Retaliation Policy (1436), and state or federal law;
 - 6.7.2.8 Violates City Policy relating to "Political Activities" (e.g. Policy 1423);
 - 6.7.2.9 Violates the city's Code of Ethics or any other applicable City Policy or Regulation governing behavior.
 - 6.7.2.10 Contains information or materials that are not releasable under public records laws or that may tend to compromise the security of City networks or information systems. This includes content that is

confidential or “for official use” documents, information 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, personal identification information, and malware. “Confidential Information” does not include terms and conditions of employment;

6.7.2.11 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 Director of Communications or his/her designee who, in turn, shall consult with the City Attorney as necessary.

6.8 Security

6.8.1 Authorized Users must be mindful of security and 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.

6.8.2 In order to minimize the possibility of security or confidentiality breaches of City Social Media Accounts, Authorized Users must:

6.8.2.1 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. Training programs and frequency will be created by the Director of Communications or his/her designee and is mandatory for all Authorized Users to complete.

6.8.2.2 Each Authorized User must print, read, and initial the terms of use and privacy controls (if applicable or available) for each account that the Authorized User manages in compliance with Section 6.2.5(b) of this policy. This is to ensure compliance and protect the security of City Social Media Accounts.

6.8.2.3 Not allow another person to utilize the Authorized User’s credentials or log-in information to manage a City Social Media Account post/publish content on the City Social Media Account

6.8.3 Passwords- To prevent unauthorized users access to City Social Media Accounts, each Authorized User shall follow City Policies (e.g. Electronic Communication Policy 1311) and any procedures established by the Director of Communications or his/her designee as related to passwords.

6.8.4 Departments with City Social Media Accounts shall provide the Director of Communications, or his/her designee, with log-in information, including username and password, for the account. The Director of Communications or

his/her designee will keep a list of account access information for immediate access to the Department-run City Social Media Accounts to ensure compliance with the security and integrity of the City Social Media Accounts.

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. The Communications Department will be responsible for any retention or dissemination of public records within their City Social Media Accounts and compliance with the applicable record management laws and policies of the City.

Any City Officers, departments, boards, commissions, committees, authorities, volunteers and employees that maintains a privately held or maintained account that that is not approved and managed in accordance with this policy and through the Communications Department is subject to a records request will be the custodian of those records and will be responsible for the archival and retrieval of those records.

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 VIOLATIONS:

Department heads shall be responsible for compliance and enforcement of this Policy within their Departments and for any Volunteers with their department. The Director of Communications or his/her designee shall be responsible for compliance and enforcement of this Policy with respect to City Officers and Volunteers not associated with a specific department.

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.