McCLOUD COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: **Social Media Use, MCSD - Fire Department - Library**
POLICY NUMBER: **3420**
ADOPTED: **March 28, 2016**
REVIEWED: **March 6, 2016, January 21, 2020**
REVISED: **February 10, 2020**

3420.10 McCloud Community Services District has a need to augment traditional communication methods with the use of social media channels. The use of social media presents opportunity and risk to the District. In general, the District supports the use of social media to further District missions and goals. The District endorses the secure use of social media technology to enhance communication, collaboration and information exchange; streamline processes; and foster productivity improvements. However, their application must not compromise data confidentiality and integrity. The same standards of conduct, principles and guidelines that apply to McCloud Community Services District employees in the performance of their assigned duties apply to employee social media technology use. This document establishes District social media use policies, protocols and procedures intended to mitigate associated risks from use of this technology where possible.

3420.20 Definitions

3420.21 Social Media. The U.S. Government defines social media as the various activities that integrate technology, social interaction, and content creation. Through social media, individuals or groups can create, organize, edit or comment on, combine, and share content. Social media uses many technologies and forms, including social-networking, blogs, wikis, photo–sharing, video–sharing, podcast, social bookmarking, mash-ups, widgets, virtual worlds, microblogs, Facebook, Really Simple Syndication (RSS) and more. Not all forms of social media may be appropriate for use by the District.

3420.21 Official District Email Account. Email account provided by the District mail system or approved external mailbox that is used for official District business.

3420.22 Approved District Social Networking Site. Approved District social networking site refers to social networks that the General Manager and the District's Information Services and Technology (IST) Provider have assessed and approved for use by District the Districts.

3420.23 Post. An administrator submitted message/blog in the form of, but may not be limited to, text, videos, photographs, graphics, links (hyperlinks), documents, computer applications, etc.

3420.24 Comment. A user submitted response to an administrator post.

3420.30 Responsibility

3420.31 The General Manager or his/her designee, are responsible for facilitating this policy in compliance with established Board policies and procedures. This includes responsibility to audit the District use of social media and enforce policy compliance.

3420.32 Social Media Coordinator. A Social Media Coordinator may be appointed by the General Manager, with authority to use social media on behalf of the District, Fire Department and Library and responsibility to ensure the appropriateness of content.

3420.40 Procedures

3420.41 District Social Media Technology Use. District use of social media technology shall conform to the policies, protocols and procedures contained, or referenced, herein.

3420.411 Comply with all applicable federal, state, and District laws, regulations and policies. This includes adherence to but may not be limited to established laws and policies regarding copyright, records retention, Freedom of Information Act (FOIA), California Public Records Act, First Amendment, Americans with Disabilities Act (ADA), Health Insurance Portability and Accountability Act (HIPAA), Hatch Act of 1939, privacy laws, employment related laws, plus District established Policies and Procedures.

3420.42 Requirements for District's use of Social Media

3420.421 Establish a well thought out social media work plan that complements District wide policies and considers the District's mission and goals, audience, legal risks, technical capabilities, security issues, emergency response procedures, etc.

3420.422 The General Manager shall be the Social Media Coordinator or shall appoint one that is responsible for overseeing the District's social media activity, policy compliance, and security protection.

3420.43 Authorized Use. The General Manager or designee, is responsible for designating appropriate levels of use.

3420.431 Social media network usage shall be limited only to those with a clear business purpose to use the forum.

3420.432 Appropriate usage levels include identifying what sites the individual is approved to use, as well as defining capability: publish, edit, comment or view only.

3420.433 Only the General Manager, Public Information Officers or appointed Social Media Coordinators, shall be considered authorized users and have permission to post and respond.

3420.434 Authorized users shall review the District's social media policies and procedures and are required to acknowledge their understanding and acceptance of their scope of responsibility via signing an acknowledgement form.

3420.44 User Behavior. The same standards, principles and guidelines that apply to McCloud Community Service District employees in the performance of their assigned duties apply to employee social media technology use.

3420.441 Authorized users shall do so only within the scope defined by the General Manager or Social Media Coordinator and in compliance with all District policies, practices and user agreements and guidelines.

3420.442 Authorized social media spokespersons participating in social networking discussions related to District business matters in off-District time shall indicate that viewpoints are personal and do not necessarily reflect District opinion.

3420.443 Violations of this policy shall be reviewed on a case-by-case basis and may result in appropriate disciplinary actions.

3420.45 Approved Social Media Networks. The Districts shall only utilize District approved social media networks for hosting official District social media sites.

3420.451 New social media networks under consideration will be reviewed and approved by the General Manager with consultation from the District's IST Provider when appropriate.

3420.452 For each approved social media network, usage standards will be developed to optimize government use of the site.

3420.453 The Social Media Coordinator may request review and approval of additional social media networks to the General Manager as needed.

3420.46 Authenticity Establishment. District social media sites shall be created and maintained with identifiable characteristics of an official District site that distinguishes them from non-professional or personal uses.

3420.461 District social media network accounts shall be created using an official District email account.

3420.462 Contact information should display an official District email address, include something about being the "official account", and provide a link to the District or the District website.

3420.463 The name "McCloud Community Services District" or the official District logo must be displayed.

3420.464 Link (hyperlink) to § 3420.475: McCloud Community Services District Social Media User Responsibility Guideline must be displayed.

3420.47 Site Content. The General Manager and/or Social Media Coordinator are responsible for establishing and maintaining content posted to the District's social media sites.

3420.471 The General Manager and/or Social Media Coordinators shall review site activity daily for exploitation or misuse.

3420.472 Social media content shall fully comply with all of the District's Personnel Policies.

3420.473 Contents posted on District social media sites may be considered public records subject to disclosure under California's Public Record Act ("PRA" – Government Code §§ 6250 et. seq.). PRA requests for the production of posts on a District social media site may be referred to District Counsel for review and response.

3420.474 Sites shall provide a link to the McCloud Community Services District Social Media User Responsibility Guideline (see § 3420.475) and, if needed, consult with District Counsel to develop the District specific disclaimers to meet the District's legal needs.

3420.475 Following forms of content posted by external and authorized users may be subject to removal if they contain:

3420.4751 Profane language or content;

3420.4752 Content that promotes, fosters or perpetuates discrimination of protected classes;

3420.4753 Sexual harassment content;

3420.4754 Solicitations of commerce or advertisements including promotion or endorsement;

3420.4755 Promotion or endorsement of political issues, groups or individuals;

3420.4756 Conduct or encouragement of illegal activity;

3420.4757 Information that may tend to compromise the safety or security of the public or public systems;

3420.4758 Content intended to defame any person, group or organization;

3420.4759 Content that violates a legal ownership interest of any other party, such as trademark or copyright infringement;

3420.4760 Making or publishing of false, vicious or malicious statements concerning any employee, the District or its operations;

3420.4761 Violent or threatening content;

3420.4762 Disclosure of confidential, sensitive or proprietary information;

3420.4763 Advocating for alteration of hours, wages, and terms and conditions of employment (applies to District employees only).

3420.477 Unacceptable content and repeat individual violators shall be removed. Contact District Counsel on any legal issues. See § 3420.48 concerning content management and deletion.

3420.478 The District shall have preventative measure in place against potential destructive technical incidents. See § 3420.49 on network security.

3420.48 Records Management. The District use of social media shall be documented and maintained in an easily accessible format that tracks account information.

3420.481 The General Manager and/or Social Media Coordinator are responsible for the creation, administration and deactivation of social media accounts

3420.482 All content is to be fully accessible to any person requesting documents from the social media site.

3420.483 Content deemed inappropriate per § 3420.475 or technically destructive per § 3420.49 shall be promptly documented (screenshot/printout), saved pursuant to District policies and procedures regarding record retention, and then be removed immediately. Contact District Counsel on any legal issues.

3420.484 Individuals (e.g., friends, fans or followers) who continue to post inappropriate content shall be removed.

3420.49 Network Security. The District shall have security controls in place to protect District information and technology assets against potential destructive technical incidents.

3420.491 Perceived or known compromises to the District's internal network shall be promptly reported to the District's IST Provider.

3420.492 Computers, laptops and mobile devices used to administer District social media sites shall have up-to-date software to protect against destructive technical incidents, including but may not be limited to, cyber, virus and spyware/adware attacks.