Fallbrook Regional Health District	Policy #____	Page 1 of 5
	Title: Social Media Policy	
Policies and Procedures Manual	Latest Revision Date: 4/11/2018	

SOCIAL MEDIA POLICY

Fallbrook Regional Health District (the "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 the exchange of information; streamline processes; and to foster productivity improvements. However, their application must not compromise data confidentiality and integrity. The same standards of conduct, principles and guidelines that apply to the District employees in the performance of their assigned duties apply to employee social media technology use. This policy establishes District social media use policies, protocols, and procedures intended to mitigate associated risks from use of this technology where possible.

Definitions:

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, podcasts, social bookmarking mash ups, widgets, virtual worlds, microblogs, Really Simple Syndication (RSS), and more. Not all forms of social media may be appropriate for use by the District.

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

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

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.

Comment. A user submitted response to an administrator post.

Responsibility:

The CEO or their designee are responsible for facilitating this policy, in compliance with established Board policies and procedures. This includes responsibility to audit the District's use of social media and to enforce policy compliance.

Social Media Coordinator. A Social Media Coordinator may be appointed by the CEO, with authority to use social media on behalf of the District and to be responsible to ensure the appropriateness of the content.

Procedures:

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

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.

Requirements for District's Use of Social Media:

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.

The CEO 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.

Authorized Use: The CEO or designee is responsible for designating appropriate levels of use.

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

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

Only the CEO or appointed Social Media Coordinator(s) shall be considered authorized users and have permission to post and to respond.

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.

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

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

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.

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

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

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

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

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

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.

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

Contact information should display an official District email address, include a statement saying it is the "official account," and provide a link to the District's website.

The name "Fallbrook Regional Health District" and/or the official District logo must be displayed.

Link (hyperlink) to the District's Social Media Policy must be displayed.

Site Content. The CEO and/or Social Media Coordinator(s) are responsible for establishing and maintaining content posted to the District's social media site(s).

The CEO and/or Social Media Coordinator(s) shall review site activity daily for exploitation or misuse.

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

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.

Sites shall provide a link to the District's Social Media policy and, if needed, consult with District Counsel to develop specific disclaimers to meet the District's legal needs.

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

- Profane language or content;
- Content that promotes, fosters, or perpetuates discrimination of protected classes;
- Sexual harassment content;
- Solicitations of commerce or advertisements, including promotion or endorsement;
- Promotion or endorsement of political issues, groups, or individuals;
- Conduct or encouragement of illegal activity;
- Information that may tend to compromise the safety or security of the public or public systems;
- Content intended to defame any person, group, or organization;
- Content that violates a legal ownership interest of any other party, such as trademark or copyright infringement;
- Making or publishing of false, vicious, or malicious statements, concerning any employee, the District, or its operations;

- Violent or threatening content;
- Disclosure of confidential, sensitive or proprietary information;
- Advocating for alteration of hours, wages, and/or terms and conditions of employment (applies to District employees only).

Unacceptable content and repeat individual violators shall be removed. Contact District Counsel on any legal issues.

The District shall have preventative measures in place against potential destructive technical incidents.

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

The CEO and/or Social Media Coordinator(s) are responsible for the creation, administration, and deactivation of social media accounts.

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

Content deemed inappropriate or technically destructive 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.

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

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

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

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 not limited to, cyber, virus, malware, and spyware/adware attacks.