Definitions

Anonymous content: A comment, reply, or post submitted to a {COMPANY-NAME} or affiliate site where the user has not registered and is not logged into the site

{COMPANY-NAME} Official: is identified as any employee, officer, Board of Director, or volunteer

Facebook: A free social networking website

LinkedIn: A social networking site designed specifically for the business community

Microblogging: A web service that allows the subscriber to broadcast short messages to other subscribers of the service

Social Media: A form of interactive online communication in which users can generate and share content through text, images, audio, and/or video. For purposes of this policy, "Social Media" includes, but is not limited to, online blogs, chat rooms, personal websites, and social networking sites, such as Facebook, Twitter, MySpace, LinkedIn, YouTube, etc. The absence of, or lack of, explicit reference to a specific social networking tool does not limit the extent of the application of this policy. As new online tools are introduced, this policy will be equally applicable without advance notice.

Twitter: A free social networking microblogging service that allows registered members to broadcast short posts called tweets

YouTube: A video-sharing website on which users can upload, share, and view videos

Overview

The use of external social media (i.e. Facebook, LinkedIn, Twitter, YouTube, etc.) within organizations for business purposes is increasing. {COMPANY-NAME} faces exposure of a certain amount of information that can be visible to friends of friends from social media. While this exposure is a key mechanism driving value, it can also create an inappropriate conduit for information to pass between personal and business contacts. Tools to establish barriers between personal and private networks and tools to centrally manage accounts are only beginning to emerge. Involvement by the IT Department for security, privacy, and bandwidth concerns is of utmost importance.

Purpose of Using Social Media

- **Building a positive image**: {COMPANY-NAME} can use social media to promote a positive image. While this is particularly important for organizations generally vulnerable to negative press or consumer discontent, it can also be used to boost {COMPANY-NAME}'s image within the community.
- **Increasing mind share**: Social media can reach large audiences at very low monetary cost, giving {COMPANY-NAME} another medium for promotion and increasing awareness of {COMPANY-NAME}.
- **Improving member satisfaction**: Members who receive more timely and personal service, in the medium that they prefer, will be more satisfied.
- **Gaining member insights**: Social media can be used to monitor public opinion about {COMPANY-NAME}, its products and services, or its competitors.

- **Increasing member retention**: Using social media builds affinity and loyalty since members are engaged using a medium, they prefer – something {COMPANY-NAME} needs to offer to remain competitive.
- **Increasing revenue**: Use of social media to create custom network applications (a.k.a. plug-ins) for product promotion or integration with {COMPANY-NAME}'s online services.
- **Member acquisition**: Use of social media to quickly and efficiently respond to member service issues. The answer to the problem can be public, making it searchable by other members who have the same request.
- **Disaster Recovery**: Use of social media to quickly and efficiently eliminate fears and communicate accurate information regarding recovery actions in the event of a disaster.

Policy Detail

{COMPANY-NAME} encourages the use of social media as a channel for business communication, consistent with BCHHU's corporate marketing and communications strategy. It is the policy of {COMPANY-NAME} to establish guidelines for safe social media usage with respect to protecting {COMPANY-NAME} information. The safety and confidentiality of information is vital to {COMPANY-NAME}'s success. {COMPANY-NAME} has established this policy to set parameters and controls related to {COMPANY-NAME} Official's usage of social media websites.

Terms and Conditions of Use

All requests for a {COMPANY-NAME} Official's use of external social media, on behalf of {COMPANY-NAME}, must be submitted to the Senior Management Team. {COMPANY-NAME} may allow access to select pre-approved social media websites. {COMPANY-NAME} Officials may only access these sites in a manner consistent with {COMPANY-NAME}'s security protocols and {COMPANY-NAME} Officials may not circumvent IT Security protocols to access social media sites.

Use of personal social media accounts and user IDs, for {COMPANY-NAME} use, is prohibited.

Use of {COMPANY-NAME} social media user IDs, for personal use, is prohibited. Use of {COMPANY-NAME} email addresses to register on social networks, blogs, or other online tools utilized for personal use is prohibited. Examples of prohibited use of company User IDs include:

- Downloading and installing plug-ins or helper applications such as those that try to access the {COMPANY-NAME} e-mail directory
- Joining groups using a company user ID for personal reasons
- Adding personal friends to a {COMPANY-NAME} Official's friends list

{COMPANY-NAME} Officials are to acknowledge they have reviewed the social media service's Terms of Service (TOS) or Terms of User (TOU), as applicable. Links for sites are below.

- Facebook: https://www.facebook.com/terms.php
- LinkedIn: http://www.linkedin.com/static?key=user_agreement
  Twitter: http://twitter.com/tos
- YouTube: http://www.youtube.com/t/terms

Representing {COMPANY-NAME}

{COMPANY-NAME} Senior Management will designate a person or team to manage and respond to social media issues concerning {COMPANY-NAME} and will determine who will have the authority to contribute content. This person(s)'s responsibilities will include, but are not limited to:

- **Managing** social media tools and channels;
- **Responding** to questions internally and externally about the social media site;
- **Addressing** problems/providing direction for staff if a user becomes threatening, abusive, or harassing;
- **Suggesting** changes to this {COMPANY-NAME} social media policy when warranted;
- **Working** with other staff to make sure opportunities aren't overlooked in marketing {COMPANY-NAME} services; and
- **Training** staff to ensure they understand how to use {COMPANY-NAME}'s social media program.

{COMPANY-NAME} will take the necessary steps to make sure the content complies with applicable laws and regulations.

All {COMPANY-NAME} Officials who participate in social media, on behalf of {COMPANY-NAME}, are expected to represent {COMPANY-NAME} in a professional manner. Failure to do so could have negative impact on {COMPANY-NAME} and could jeopardize a {COMPANY-NAME} Official's ability to participate in social media in the future.

{COMPANY-NAME} owns all authorized social media and networking content. {COMPANY-NAME} Officials are prohibited from taking, saving, or sending any {COMPANY-NAME} content distributed via social media while employed, separated, serving on the Board of Directors, or terminated by {COMPANY-NAME}.

New technologies and social networking tools continually evolve. As new tools emerge, this policy will be updated to reflect the changes.

Platforms for online collaboration are fundamentally changing the work environment and offering new ways to engage with members and the community. Guiding principles for participating in social media should be followed.

- Post meaningful, respectful comments and refrain from remarks that are off-topic or offensive.
- Reply to comments quickly when a response is appropriate.
- Know and follow the state and federal laws that protect member confidentiality at all times.
- Protect proprietary information and confidentiality.
- When disagreeing with others' opinions, keep it professional.
- Know the {COMPANY-NAME} Code of Conduct and apply the standards and principles in social computing.

Personal Blogs and Posts

{COMPANY-NAME} takes no position on a {COMPANY-NAME} Official's decision to start or maintain a blog or personal website or to participate in other online social media activities outside of work. {COMPANY-NAME} Officials, identifying themselves as a {COMPANY-NAME} Official on a social network, should ensure their profile and related content is consistent with how they and {COMPANY-NAME} wish for them to present themselves. This includes what the {COMPANY-NAME} Official writes about himself/herself and the type of photos he/she publishes.

{COMPANY-NAME} Officials must not reveal proprietary information and must be cautious about posting exaggerations, obscenities, or other characterizations that could invite litigation.

{COMPANY-NAME} Officials must not make public reference to any {COMPANY-NAME} related cash or security procedures.

{COMPANY-NAME} Officials who comment on any {COMPANY-NAME} business or policy issue must clearly identify themselves as a {COMPANY-NAME} Official in their blog or posting and include a disclaimer that the views are their own and not those of {COMPANY-NAME}. When generating content that deals with {COMPANY-NAME} or individuals associated with {COMPANY-NAME}, {COMPANY-NAME} Officials should use a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of {COMPANY-NAME}".

{COMPANY-NAME} Officials must not use social media websites to harass, threaten, discriminate against, disparage, or defame any other {COMPANY-NAME} Officials, members, vendors, {COMPANY-NAME} products, services, or business philosophy.

{COMPANY-NAME} Officials are prohibited from disclosing confidential, proprietary, or otherwise sensitive business or personal information related to {COMPANY-NAME} or any of its {COMPANY-NAME} Officials, vendors, or members. {COMPANY-NAME} Officials are also prohibited from disclosing any confidential, proprietary, or otherwise sensitive business or personal information that could identify another {COMPANY-NAME} Official, vendor, or member without that individual's prior authorization.

{COMPANY-NAME} Officials should not take any action via social media websites or personal blogs that would harm, or is likely to harm, the reputation of {COMPANY-NAME} or any {COMPANY-NAME} Officials, members, or vendors.

Rules of Engagement

Protecting member information is everyone's number one responsibility. Information that can be used to disclose a member's personal information in any way should never be posted. Members trust {COMPANY-NAME} to protect their financial assets and information.

Communications in written, audio, or video form will be around for a long time, so consider the content carefully and be judicious. Brand, trademark, copyright, fair use, and privacy laws must be respected. If any employee mentions a financial product in a blog, a tweet, or another form, financial disclosure laws apply online. The employee must comply with advertising disclosure regulations by providing a link back to {COMPANY-NAME}'s website page that lists the proper disclosures.

What is written, produced, or recorded is ultimately the employee's responsibility. Participation in social computing on behalf of {COMPANY-NAME} is not a right and, therefore, needs to be taken seriously and with respect. Failure to comply could put an employee's participation at risk and can lead to discipline. Third-party site's terms and conditions must be followed.

Denigration of competitors, {COMPANY-NAME}, or {COMPANY-NAME} affiliates is not permitted. Communication should be respectful when inviting differing points of view. Topics like politics or religion are not appropriate for {COMPANY-NAME} communications. Communicate carefully and be considerate; once the words or other materials are out there, they cannot be retracted.

Personal information belongs to the members of {COMPANY-NAME}. It is their choice to share that information, not {COMPANY-NAME}'s. {COMPANY-NAME} will not publish material without first discussing it with a manager or legal representative.

Rules of Composition

- {COMPANY-NAME} Officials should write and post about their areas of expertise, especially as it relates to {COMPANY-NAME}.
- Write in the first person. Talk to the reader as if he/she were a real person in a professional situation.
- Avoid overly composed language.
- Consider content that is open-ended and invites response.
- Encourage comments.
- Use a spell-checker.
- Make the effort to be clear, complete, and concise in the communication. Determine if the material can be shortened or improved.

- If a mistake is made, it must be acknowledged. Be upfront and be quick with the correction. If posting to a blog, make it clear if a modification has been done to an earlier post.

Produce material {COMPANY-NAME} members will value. Social media communication from {COMPANY-NAME} should help its members, partners, and co-workers. It should be thought

provoking and build a sense of community. It should help members improve their knowledge or understand {COMPANY-NAME} or an affiliate better.

Anonymous content is not allowed on {COMPANY-NAME} sites.

Personal Use of Third-Party Sites During Work Hours

E-mail and Internet access is provided to support {COMPANY-NAME} business purposes. If these tools are accessed, incidental personal use of them is permitted. In general, {COMPANY-NAME} will limit the access of social media sites to {COMPANY-NAME} Officials who use it on behalf of {COMPANY-NAME}. Excessive personal use of any Internet tool during work time is not permitted and access privileges may be revoked for abuse of the system.

Retaliation is Prohibited

{COMPANY-NAME} prohibits taking negative action against any {COMPANY-NAME} Official for reporting a possible deviation from this policy or for cooperating in an investigation. Any {COMPANY-NAME} Official who retaliates against another {COMPANY-NAME} Official for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination of employment at {COMPANY-NAME} or removal from the Board of Directors.