Cisco College Social Media Guide

1. Introduction

These guidelines and policies are intended to assist College employees who will use social media as a communication tool to encourage social media use between the college, students, faculty, staff and the community. Given the evolving nature of social media, this document will be reviewed and updated periodically as technologies or laws evolve.

2. Purpose

Social media offers Cisco College the opportunity to interact with the public in new, exciting ways that facilitate transparency, interactivity and collaboration. These tools engage audiences differently than traditional media and enhance communication strategies.

Cisco College encourages the use of social media to advance the goals of the college and the missions of its departments, where appropriate.

The purpose of this guide/policy is to assist the employees of Cisco College in effectively and responsibly navigating issues unique to social media. This includes the management and development of social media tools, content, restrictions and limitations.

The definition of social media is web-based applications that facilitate information sharing and collaboration such as web-based communities, social networking sites, video-sharing sites, wikis, blogs and others.

Authorized employees who are responsible for developing, maintaining and monitoring social media applications should be designated by the Director of Marketing and Public Relations. Individuals outside of The Office of Marketing and Public relations seeking to publish content any of the Cisco College social media networks shall seek approval from the Director of Marketing and Public relations prior to publishing.

3. Applicability

These guidelines and policies are applicable to all Cisco College employees, elected and appointed officers, and officials who utilize any social media directly or indirectly on behalf of the college. This policy also applies to all college personnel who personally utilize any social media or other Internet activity that may impact the college's credibility, reputation, employee morale, service, or goals of Cisco College.

These guidelines apply without regard to whether the use of social media occurs during working or non-working time, or on duty or off duty use. Similarly, the policy applies regardless whether college equipment or college time is used.

4. Acceptable Uses and Restrictions

The best and most appropriate uses of social media for Cisco College generally fall in two categories:

- As a channel for disseminating time-sensitive information as possible.
- As a mechanism for communication between Cisco College, students, faculty, staff and the community.

College staff representing Cisco College on affiliated college social media sites and applications in the course of their assigned duties and responsibilities are bound by existing college policies and standards, including but not limited to:

- Applicable state, federal and local laws, regulations, ordinances, charter provisions and college policies;
- All information and technology security guidelines, procedures and policies;
- Existing College standards of conduct, ethics, rules and policies;
- The Texas Public Information Act and e-discovery laws and policies;
- Applicable state records-retention laws and college schedules for retention.

Personal Responsibility

All college employees must be cognizant that how they present themselves on social media applications reflects on the college whether with respect to college social media sites or personal ones.

In all applications, the following shall apply:

Confidentiality

Employees will not post or use proprietary, confidential, sensitive or individually identifiable information or divulge college intellectual property (trademarks, copyrights, or patents) in any social media applications.

Disclaimers

If employees refer to or identify themselves as college employees on social media applications, use of a disclaimer is mandatory. (E.g. “While I work for Cisco College, anything I publish is my personal opinion and not the opinion or position of Cisco College, or a reflection of the college’s policies.”)

Personal vs. Professional Use
Employee’s personal social media sites should remain personal in nature and should not be commingled or used for work-related purposes or to conduct official college business.

Use of College Resources
Employees may use college owned assets and equipment or resources to access social media sites (personal or professional) on a limited basis. Department directors will determine the level of access assigned to authorized users and the limits of non-business use in their respective departments.

E**thical Obligations**
College ethical rules must be followed at all times, even when employees engage in social media use in their personal capacities.

Professional Responsibility

All college related communication through social media applications should remain professional in nature and should be conducted in accordance with the college’s communications policy, practices and expectations. Employees are expected to use good judgment and take personal and professional responsibility for any content they publish via social media.

All employees who use social media applications must:

Authorization
Not access social media sites or other online forums on behalf of the college unless authorized by appropriate college management. Program directors and department chairs are authorized to create and manage social media accounts for their respective programs. Login information must be shared with the Director of Marketing and Public Relations.

Identify Yourself Clearly
When creating or using social media accounts that require individual identification, authorized speaking on behalf of the college should identify themselves, if possible, by: 1) full name; 2) title; 3) department; and 4) contact information, when posting or exchanging information on social media forums.

Unauthorized use of an authorized employee's identification or access credentials/ information is a violation of this policy and will be disciplined accordingly.

No Privacy Expectation
Employees should have no expectation of privacy as to information stored on college computers, networks, databases or devices. Furthermore, there should be no expectation of privacy regarding any communications between any college employee and the public when the employee is in course and scope of performing his/her assigned duties.

Authorized Use
Only authorized college employees may moderate college developed social media applications and sites on behalf of the college. Authorized employees must support the college's missions and goals in doing so.

Communication Quality

Authorized employees should use good judgment and accuracy in all college social media communications. Errors and omissions reflect poorly on Cisco College and may result in liability for the college. In addition to the Professional Responsibilities listed above, authorized college staff should refrain from any social media activity that is inconsistent with, or that reasonably could be expected to negatively impact Cisco College's reputation or standing in the community. Employees are cautioned to be respectful and professional to everyone, including fellow personnel, organizations, residents and businesses.

When drafting a communication, make sure that it:

- Has a clear purpose
- Speaks well to the reader
- Is clear and concise without unnecessary verbiage or jargon
- Provides value to the reader
- Uses proper spelling, grammar, syntax and punctuation
- Is positive and informative
- Offers links, pictures or references opportunities for more information where reasonable.
- Has benefit to both the college and public

In addition to the suggestions listed above, best practices on how to be a good citizen of the social media environment include:

Be Responsible
All statements made about the college on any social media site, whether personal, private or official, reflect upon the college, its employees, services and elected officials. Each employee will be held accountable for all posts made officially on college media sites or personally on college media sites or on personal social sites. Once published, a communication can never be totally eliminated from the web, even if withdrawn. Defamatory or disparaging statements about the college, its agents, employees or services made on personal or private social media sites are no less a reflection on the college and serve as a basis for lack of accountability against any employee who violates these guidelines.

Be Honest and Transparent
Dishonesty, deceit and untruthfulness are quickly notes in the social media environment and have a deleterious effect on the college. Therefore, all representations made on college media sites must be clear, accurate, complete, thorough and truthful.

Correct Errors Quickly
Any mistakes should be admitted as directly feasible. Omissions, misleading entries or misrepresentations must be corrected as soon as they are recognized or brought to the college's attention. Correct information will be quickly provided with appropriate modifications and disclaimers, if necessary or helpful, to clear up any misunderstanding or confusion.

Be Respectful of the Reader and the Audience
Social media publications should only be made when the college and or the public would benefit from the publication. Value MUST be added. Communications from the college should assist the public and build a co-beneficial relationship and rapport with the college and its agents. This could include, among other things, thought provoking articles that build a sense of community, improve knowledge or skills, increase brand recognition, encourage enrollment, increase awareness of college resources and encourage mutually beneficial platforms for employees to provide better, more efficient services.

Stay Within Your Area of Expertise or Authority
All information posted on college sites must be authorized and appropriate. Employees should only publish information within their own area of expertise and

not speculate, guess or assert personal opinion or commentary unless appropriate management grants approval.

Respect Proprietary information, Content, Privacy and Confidentiality
For any non-original work, proper credit must be attributed. No copyrights, trademarks, trade secrets or other proprietary matter may be published without prior written approval, licenses obtained, permits and fees paid and/or proper attribution made within the publication itself. Links may be referenced to other's work rather than reproducing it. Employees' or officials' names and/or likenesses may be used only with permission from such person to post on the site. All publications that include college intellectual property of any kind must be safeguarded with appropriate disclaimers and notices to prohibit the unauthorized use or performance of such proprietary matters.

Respond Quickly
All communications requiring a reply or response shall be made in a timely manner in accordance with these guidelines.

Be Sociable, Courteous and Respectful
In all communications, employees should use plan language and avoid using jargon or acronyms. Use content that is open-ended and invites a response or encourages comments. Responses should always be polite and respectful, even if the original response is not. When shortening words to maximize communication, utilize common shorthand terms, letters and symbols.

Abide by Social Media Rules
Employees utilizing social media sites shall abide by the site's terms of service or terms of use. Before utilizing the site, each employee shall become acquainted with each site's terms and conditions of use or rules for services and follow them as directed. No employee is authorized to abuse a social media site and shall be held accountable for any abuse, misuse or violations of such terms or rules of engagement. Reminder: Users must seek approval from the Director of Marketing and Public Relations prior to publishing content to Cisco College social media networks.

Prioritize your Participation
Authorized employees shall use social media sites only as approved and should not linger longer than necessary. Duration of use shall be commensurate with job

duties and responsibilities and only as long as necessary to complete college business.

Photo Guidelines

Users are encouraged to use social media to show photographic updates on what is going on in their departments and with special events. During college events, users are should feel free to post one or two photos to capture the event and use proper tagging and hash tagging when applicable. Users should not post large albums to the College social media channels without approval from the Director of Marketing & Public Relations. When using a smartphone to capture a photo, the user should always use the camera in landscape mode (horizontal) or if the camera app has a square photo feature, use that. Do not take vertical photos.

Things to remember when taking a photo:

- Make sure your subject is well lit.
- Make sure your subject is in focus.
- Try to capture the faces of your subject.
- Photos of your subject in action are best.

For any photo posts that do not fall under the classification of "in-the-moment" event posts, they should be sent to the Director of Marketing & Public Relations for review, approval, and proper branding before posted.

Restrictions and Prohibitions

Users and visitors to Cisco College social media sites will be notified that the intended purpose of the site is to serve as a mechanism for communication between Cisco College and the public. Although free speech and cross-communication is encouraged, there are certain topics and issues that are NOT allowed on Cisco College social media sites comments, links and uploads. By way of example, these include, but are not limited to:

- Comments in support of or opposition to political campaigns or ballot measures
- Profane language or content. Abusive or disparaging comments directed at individual(s).
- Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status or lack thereof, socio-economic status of individual(s), national origin, physical or mental disability or sexual orientation

- Content that my show or could be interpreted to be cruelty to animals or any living creature.
- Sexual expression, discrimination, harassment or content of any kind or links to sexual content or pornography whether of an adult, minor or child.
- Any expression of conduct or encouragement of illegal activity
- Information that may tend to compromise the safety or security of the public or the college's public safety systems
- Any expression of words that would disparage right, title or interest of a legal ownership of any other individual or business.
- Comments that do not pertain to the topic under discussion; including comments containing links to other websites or pages which are not relevant to the topic under discussion
- References to or inappropriate characterizations of individuals including personal attacks upon any member of the public, college employee or college official.
- Advertising or promotional announcements of private or commercial enterprises, even if not for profit unless the college is co-sponsoring such activity or event. Only college business related advertising (services) or promotional announcements (special events) are allowed.
- Individually identifiable information (e.g. address, phone number and social security numbers) of specific individuals be they college employees, officials or members of the public.

Cisco College reserves the right to restrict or refuse to re-publish any content that is deemed in violation of these guidelines or any applicable federal, state or local law(s), including the terms of service or terms of use outlined by third-party social media application providers. Cisco College reserves the right to block users who violate these terms.

Monitoring

Social media is an engaging medium and welcomes two-way and cross conversations, giving Cisco College the opportunity receive and obtain comments and feedback from users regarding how the college is perceived, what it is doing right and what users think might be wrong or done more effectively or efficiently.

Monitors enforce this policy and guidelines to ensure content and posted comments are suitable for all readers, while respecting the gamut of opinions and points of view.

Prohibited, negative and/or inappropriate comments from users are to be expected given the deeply felt passion some individuals express about topics close to their hearts. Unacceptable forms of communication should not become a worrisome issue or treated as a sign of failure in social media strategies and usages. Instead, such comments can be reformed into positive effects, indicating to the online community that the college is professional, engaged in a dialogue with its users and that it values their.

Typical scenarios with suggested outcomes – a guide:

Identify the Type of Feedback

The first step in dealing with negative feedback is determining what type of comment has been received. Negative feedback comes in a few different forms, each of which is best dealt with by a different type of response.

Constructive Criticism

Many users will use social media to suggest ways in which the college can improve. While this type of feedback may point out flaws or issues, it can be extremely helpful to receive.

Merited Condemnation

Essentially, Cisco College or one of its agents did something wrong, and someone is unhappy. Again, while this type of feedback is not positive, it can serve as a means to convey information regarding solutions being worked, results achieved and ways that issues have been resolved.

Trolling/Spam

Trolls and spammers will use a negative comment about the college, a political figure or provided service (whether true or false) to promote a competing entity, person or service.

Determine Best Approaches for Response

When responding to criticism, even the negative type, it is important to stay positive. Adding more negativity to the conversation or being drawn into a fight with a customer or user will likely reflect poorly on the organization.

Constructive Criticism

A response is almost certainly necessary. Regardless, if a real problem exists, steps should be taken to remedy the issue, therefore it is important communication occurs between the social media moderator and department handling the problem. Sometimes, this type of feedback is the

result of a perceived problem rather than an actual problem (e.g. someone who doesn't like the method by which something was done). This type of complaint should be given a response, if only to say, "Thank you for bringing it to our attention, but here is why we have this procedure in place."

There will be times when the organization will not want to implement the suggestion given, however, trust will be built by responding to criticism with a positive message.

Merited Condemnation

This can be tougher to deal with, because comments are more likely to feel personal. It is important to keep in mind that this type of feedback, as harsh as it may be, has a basis in a real problem. It is best to respond promptly and with a positive tone (e.g. thank the user for the feedback and assure them that steps are being taken to correct the issue or mitigate their problem).

Trolling/Spam

This is the only category of negative feedback that does not require a response. In fact, it is almost always best not to respond to these messages. This type of feedback isn't really feedback at all. It is best to ignore this variety of feedback, and when appropriate, to remove it as soon as possible from the medium and/or report the user to appropriate application support.

5. Security

College staff members need to take every caution to prevent fraud or unauthorized access to social media applications. In almost every case where an attacker accesses a system without authorization, he/she does so with the intent to cause harm, including:

- Making unofficial posts, tweets or messages that will be seen by the public as official messages.
- Encouraging users to either click links or download unwanted applications that the attacker has added to the site.
- Accessing, compromising or disabling a college system.
- Redirecting users to sites that look like a college site but are used to gather data that could be used for unauthorized purposes (e.g. phishing)
- Using a compromised site to spread malware.

- Acquiring confidential information about college employees or students (e.g. social engineering).

How to Mitigate Security Risks

Security related to social media is fundamentally a behavioral issue, not typically a technology issue. In general, employees unwittingly providing information to third parties pose a risk to the college network. Employees need to be aware of current and emerging threats that they may face using social media sites and how to avoid falling prey. The following are best practices when using social media:

- A separate user ID and password must be used to access social media sites, NEVER use your College Network username and password
- Never duplicate user IDs and passwords across multiple social media sites
- Learn more about security awareness and risks when using social media
- Ensure privacy settings are set appropriately
- Review (and apply as appropriate) patches for Firefox, Adobe and Java as these softwares can be common paths for security vulnerabilities.

6. Disclaimer

These guidelines are intended to supplement -- not replace -- Cisco College's Personnel Policies. Policies on confidentiality, controversial issues, personal use of college equipment, professionalism, references for former employees, publication of articles, unlawful harassment and other rules of conduct addressed in other policies are not affected, altered or amended by these guidelines. If not specifically addressed in this policy, an issue often can be clarified by reference to other Cisco College policies. Similarly, conduct that violates this policy will be subject to the same action as set forth in college personnel policies and may be disciplined accordingly.

7. Questions, Comments and Concerns

If, at any time, there is an uncertainty about how to apply these guidelines or questions arise regarding participation in social media, all employees are directed to seek the guidance of the Director of Marketing and Public Relations. Social media is in a state of constant change and Cisco College recognizes that there will likely be events or issues that are not addressed in these guidelines. Therefore, the responsibility falls to each individual to use good judgment, and when in doubt, to ask for clarification or authorization before engaging in questionable online conduct. Any employee who observes questionable or inappropriate social media conduct or posts whether on official college sites or on personal or private sites that could be a violation of this policy or potentially negatively impact Cisco College, are directed to report this information to the President or Director of Marketing and Public Relations.