UNK Social Media Guidelines

Philosophy/purpose

UNK will use social media strategically and purposefully to increase awareness of the University of Nebraska at Kearney and strengthen relationships with prospective students, alumni, faculty/staff, community members, Loper fans and anyone who desires a relationship with UNK.

For whom

These guidelines are suggested by UNK Marketing and University Communications and Community Relations for UNK faculty and staff in conjunction with their duties as representatives of the university on university-affiliated or branded social media networks and channels. Students, however, may find guidance applicable to their own use of social media on their personal spaces. Students who are representing UNK on university-affiliated networks, sites or channels are expected to follow these guidelines, under guidance of UNK faculty or staff.

Account Creation and administration

Any UNK social media site developed to represent or communicate for a UNK department, office, unit, college or other administrative UNK entity must be developed and led by a UNK faculty or staff member. Some social media sites will allow you to add additional administrators to help keep your community updated. We require at least two social-media-channel administrators responsible for updating content for your site. When a social media administrator leaves, this allows the remaining administrators to continue updating the site. Administrators who leave the university must be removed as administrators and passwords should be changed. If you authorize students to post or be an administrator for your UNK social media site/account/outpost, they must understand and adhere to these social guidelines.

A social media dashboard has been developed http://www.unk.edu/social
to streamline the following/signup process for our audiences. If you develop a UNK-associated social media account, notify Amanda Andresen or Thane Webb to add your account to the dashboard.

Why social media: Planning, strategy, objectives

Before developing a social media presence, it's recommended you have a plan. This can be basic or quite extensive depending on your unit's preference. At a minimum, a plan should outline: *What are we intending to create in this space* (provide information, develop and enhance relationships, share content for fun, to inform)? Objectives should be long-term and focus on outcomes and the quality of the engagement rather than numbers. If you aren't sure why you want to have a social media presence, walk through the <planning template hotlink word Doc>. You will need to have a plan for monitoring the conversations on your social sites, responding to questions and feedback. You also need a content-development plan (what you are posting, frequency, how to promote your presence on other sites, etc.) Contact Kelly Bartling or Amanda Andresen for help with your social media planning.

Integration with other university channels

Communications and Marketing has developed a social media plan, as part of the university's broader strategic communications and marketing plan. The plan outlines the top-level channels for UNK: @UNKearney and UNKearney on Facebook http://www.facebook.com/UNKearney. Leadership on content development for and deployment of content for priority events and campaigns for UNK will be by social media coordinator Amanda Andresen. Units, affiliates and individuals will be asked to integrate main-level content into their plans and share main-level content, developing their own unit-specific content. The main- level sites will likewise link to and share appropriate content from other UNK channels from the UNK dashboard. A social media working group will be developed to establish and share important events and strategic campaigns through a social media calendar. This working group, calendar and process will assure best strategic and integrated content campuswide.

Branding/appearance/naming

Any faculty, staff, department, unit, or other affiliated presence on social media that relates to the trademarked images (Louie, the UNK nameplate/icon, Lopers) that implies communication on behalf of UNK must be authorized by UNK Communications and Community Relations. No staff/faculty-targeted pages will be developed (i.e. "UNK staff Facebook" or "Loper Faculty Community") that provide forums or social networking for UNK faculty and staff without senior administrative approval, in coordination with Human Resources and Information Technology Services.

Naming Guidelines

Use the official name of your program, unit, affiliate or department that matches your UNK web page. For example, if your UNK web page lists your program as "UNK Creative Services," make sure your social media account/site is "UNK Creative Services" not "Creative Services at UNK or Loper Creative Services." Keep it consistent with the name people already recognize for your program.

Also, if using multiple social media channels, be consistent with your name across channels so it is easier for users to find you. For example, @UNKearney on Twitter and http://www.facebook.com/UNKearney

Use of University logos, colors, brand marks

Accounts and pages should, where possible, feature the program's university-approved name, logo or signature. We also encourage the use of photographs to display campus beauty, a "destination" or physical place for your program, or stylized images that portray your program.

When a social media platform allows changes to layout or design, university colors should be used.

The use of university marks, such as logos and graphics, must comply with university policy. For information about colors, typeface, size and other details, please contact Kyle Means, Director of Marketing.

Use of personal identifying images

In most cases, prior permission (a "release") must be obtained to post, share or distribute images of individuals whose images are identifiable. For that reason, it is always best to use content, such as photographs or videos, obtained by university representatives specifically for the purpose of posting or distribution.

Best practices and ideas to generate followers, quality conversations

Cross-promotion

Generate awareness of your social media community and help it grow by listing it in other publicity efforts. If you're committed to updating your social community regularly and want it to grow, you should list it everywhere you would list your program or department's website: on brochures, posters, business cards and other printed information. Visual cues to prompt audiences to find you on social media are strongly suggested (aka "chicklets.")

Be sure to include a link to your social media community wherever you list your contact info on your university web page. You may also want to consider listing it as part of your email signature. If you're trying to publicize a Facebook Page, be sure you've given it a username, so you've got a short, easy-to-list URL to include in your overall communications efforts. <example>

If you're launching a Facebook page for your program or department, visit the UNK Facebook page and add all the UNK Facebook pages listed there under "Favorite Pages" to your "Favorite Pages." Following, liking, sharing and listing other channels helps develop an integrated cross-promotional effort to maximize following and attention on all of our channels.

Managing Feedback

Actively and routinely monitor feedback on your pages. Be alert for negative dialogue. Responding to negative feedback is often more important than responding to positive feedback because of the opportunity to change someone's perception of the university and/or department. Respond only when appropriate: A response is needed when you can add value to an issue. Correct inaccurate facts. Take reasonable action to correct the issue and let the person know what has been done. About deleting or blocking: Always let the comment stand as is unless it is potentially harmful to another, is profane or inappropriate toward another's reputation. Unless the comments are of a harassing nature, make the situation unpleasant for a majority of members or are SPAM, you should not remove posts.

Contact UNK Information and Technology Services and UNK Police for concerns on threats or other concerning behavior observed in your online communities. UNK has experts here to guide us on threats and threatening behavior.

Through your social media plan, identify and carry out a routine monitoring strategy: Check your interactions on specific intervals, and know who is monitoring, who is authorized to respond, and define/describe appropriate contacts for response and follow-up. Several free alert products exist that can help you monitor your channels. Contact Amanda Andresen for ideas and suggestions.

Emergencies/Crisis communication

To ensure a consistent message and the latest information, a social media crisis communication plan has been developed.

What you need to know: the main level UNK accounts will be used during emergencies, closings and major news happenings as the first source of information. Do not attempt, in an emergency, to post information without authorization. You may be asked to deploy and help disseminate specific information to your followers at specific times, under best practices consistent with crisis communication theory and strategy. Monitoring your channels for conversations and questions will be your first step in a crisis, refraining from posting until directed by the incident's public information officer.

Best Practices for engagement

Post content that is meaningful and relevant to your organization.

Think about how the content might advance your initiatives and goals. Write in a manner that represents your entire unit. Use "we," "our" and other inclusive words. Keep content fresh. Provide regular and timely updates, but don't overdo it. Keep in mind what is appropriate for the specific social media outlet that you are using.

Interact with users. Post content that encourages feedback and positive interaction. When possible and appropriate, include visual content — photos and videos — to increase engagement. Be friendly, helpful and informative. Connect users with resources. Link back to content throughout the unk.edu website to drive traffic back to the university and your own web pages. When sharing news about your unit, provide a link to the university's news release or official announcement.

Think twice before posting. Privacy does not exist in the world of social media. Consider what could happen if a post becomes widely known and how that may reflect on both the poster and the university.

Strive for accuracy. Remember you are posting on behalf of UNK and what you post affects UNK's reputation. Ensure the information being posted is accurate and timely. Also, review content for grammatical and spelling errors. Employ a "second set of eyes" process to post, if necessary. It's always better to be accurate than having to publish a retraction later.

Be respectful. Understand that content contributed to a social media site could encourage comments or discussion of opposing ideas. Responses should be considered carefully in light of how they would reflect on the university.

Current and Timely. If you are going to have a social media site then it should be monitored and information and/or responses should be timely. If a mistake or error is posted then correct it in a timely manner and in a visible way. Saying "oops, we goofed" is often the best way to correct yourself. Don't be too dismissive but don't go overboard apologizing either.

Remember your audience. This could include prospective students, current students, employers, colleagues and peers all in the same site. Ensure that what you post will not alienate, harm or provoke any of these groups.

Be transparent. Be honest about your identity. If you are authorized by your supervisor to represent UNK in social media, say so and identify yourself appropriately. Never hide your identity for the purpose of promoting UNK through social media. The Public Relations Society of America has some useful standards and advice on social media ethics <link>.

Responsibility/regulations

As a university, we must adhere to laws and regulations relating to student privacy in addition to other "best practices." Do not post confidential or proprietary information about UNK students, staff, faculty or alumni. FERPA (the Family Educational Rights and Privacy Act) and HIPAA (the Health Insurance Portability and Accountability Act) as well as NCAA regulations. You must remember, under these regulations, students' educational information and health privacy are to be protected at all times. You may not publish grades, coursework or other information about students without their permission. Adhere to all applicable university privacy and confidentiality policies, in addition to the computer use guidelines and the faculty code of conduct (if applicable to you) AND Executive Memorandum 16. Employees who share confidential information do so at the risk of disciplinary action or termination. <Faculty Senate Professional Conduct><HR/business ethics code = http://www.unk.edu/uploadedFiles/admin/vcbf/policy/5.0/Code_Professional_Ethics_UNK.pdf>

Advertising on behalf of external vendors is prohibited on UNK social media presences (with the exception of UNK Athletics, through their media rights provider). Refer to the university guidelines and rules on using university computers and information systems – Executive Memorandum 16. <http://www.unk.edu/uploadedFiles/offices/ITS/policies/exec_memo16.pdf>.

Copyright images and fair use

Respect copyright and fair use: When posting, be mindful of the copyright and intellectual property rights of others and of the university. For guidance, consult UNK's Copyright resources page on the web: http://www.unk.edu/academics/cte/Copyright_Resources_for_Educators/

And, University of Nebraska's Memorandum on Copyright Law and Compliance: http://nebraska.edu/docs/policies/MemorandumonCopyrightLawandCompliance.pdf

Terms of service

All social media platforms have specific rules and Terms of Service. These often relate to things like identities and self-identification, contests, copyright, administration, and what is or isn't appropriate to post. Obey the Terms of Service of any social media platform employed.

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

Personal vs. professional accounts

If you also maintain your own personal social media accounts, you should avoid creating confusion over whether or not the account is associated with UNK. If you identify yourself as a UNK faculty or staff member online (even in sub-pages, "About me," or posting a photo of yourself in UNK garb), it should be clear that the views expressed on your site are not those of the university and you are not acting in your capacity as a UNK employee. UNK employees may consider adding this disclaimer to personal social media accounts: “Comments here are my own and not the university’s/UNK’s/department’s.”

University data – Posting sensitive information intended only for internal use on a social networking service can have serious consequences. Disclosing students’ private education information, draft or discussion documents, faculty intellectual property, items under negotiation, trade secrets, personnel issues, or other university, college or committee activities could result in liability or bad publicity.

Professional reputation – Inappropriate photos or content on a social networking service may threaten a user’s educational and career prospects. Many companies also perform online searches of job candidates during the interview process. Information that suggests that a person might be unreliable, untrustworthy, or unprofessional could threaten the candidate’s application.

Personal relationships – Because users can upload comments from any computer or smart phone that has internet access, they may impulsively post a comment that they later regret. Even if comments and photos are retracted, it may be too late to undo the damage. Once information is online, there is no way to control who sees it, where it is redistributed, or what websites save it into their cache.

Personal safety – You may also compromise your personal security and safety by posting certain types of information on social networking services. For example, revealing that you will be away from home, especially if your address is posted in your profile, increases the risk that your home will be burglarized. You may also risk the safety of your children by posting photos and personal details. For example, if malicious individuals are able to collect enough information, such as the child’s name, school, activities, or details about the parents, they might be able to lure a child into a dangerous situation.

Proper conduct – These guidelines affirm and reinforce UNK’s Affirmative Action/Equal Opportunity provision. Sexual harassment, as defined in these policies, http://www.unk.edu/offices/aaeo/policies/Defining_Sexual_Harassment, is prohibited. Bullying behavior or anything that interferes with another’s academic performance or creates an intimidating, hostile or offensive learning or social environment, including posts on social media, is prohibited.

Disclaimer – These guidelines not intended to interfere with employees' rights under the National Labor Relations Act. Nothing in these guidelines should be interpreted to prevent, interfere with, or otherwise restrain an individual's legitimate exercise of his or her Section 7 activities under the National Labor Relations Act. This policy does not apply to discussions or activities involving the terms and conditions of employment.

Security

When you share information online, you need to understand the potential risks, and you need to be wary of what you share and with whom.

Attacks and Unintended Information Disclosure

Attackers may use social networking services to spread malicious code, compromise users' computers, or access personal information about a user's identity, location, contact information. The following are some common threats to social networking services:

Viruses – The popularity of social networking services makes them ideal targets for attackers who want to have the most impact with the least effort. By creating a virus and embedding it in a website or a third-party application, an attacker can potentially infect computers just by relying on users to share the malicious links with their contacts.

Tools – Attackers may use tools that allow them to take control of a user's account. The attacker could then access the user's private data and the data for any contacts that share their information with that user. An attacker with access to an account could also pose as that user and post malicious content.

Social engineering attacks – Attackers may send an email or post a comment that appears to originate from a trusted social networking service or user. The message may contain a malicious URL or a request for personal information. If you follow the instructions, you may disclose sensitive information or compromise the security of your system.

Identity theft – Attackers may be able to gather enough personal information from social networking services to assume your identity or the identity of one of your contacts. Even a few personal details may provide attackers with enough information to guess answers to security or password reminder questions for email, credit card, or bank accounts.

Third-party applications – Some social networking services may allow you to add third-party applications, including games and quizzes, that provide additional functionality. Be careful using these applications—even if an application does not contain malicious code, it might access information in your profile without your knowledge. This information could then be used in a variety of ways, such as tailoring advertisements, performing market research, sending spam email, or accessing your contacts.

An important element to remember about social networking services is that users may post information about other people. Without even realizing it, you may put someone else at risk by posting a comment or photo that could compromise that person’s privacy or security. Sometimes, posting negative content about someone else is intentional. Social networking services have become channels for conducting cyberbullying, a growing problem that can lead to significant psychological trauma.

Implement Security Measures

Taking general security precautions will reduce the risk of compromise:

1. Use strong passwords, and use a unique password for each service.
2. Keep anti-virus software up to date.
3. Install software updates in a timely manner, particularly updates that affect web browsers.

Follow Good Practices

Social networking services offer unique risks, and you can minimize these risks by adopting good security practices.

1. **Use strong privacy and security settings** – Take advantage of the security options provided by social networking services. When choosing appropriate options, err on the side of privacy to better protect your information. These services may change their options periodically, so regularly evaluate your security and privacy settings, looking for changes and ensuring that your selections are still appropriate. Also periodically review the services’ privacy policies to see if there are any changes.
2. **Avoid suspicious third-party applications** – Choose third-party applications wisely. Look for applications developed by vendors you trust, and avoid applications that seem suspicious. Limit the amount of information third-party applications can access.
3. **Treat everything as public** – The best way to protect yourself is to limit the amount of personal information you post to these services. This recommendation applies not only to information in your user profile, but also to any comments or photos you post. It is important that you consider information that you post about yourself and about others, particularly children.
4. **Share only with people you know** – Although many users seek to establish as many contacts on these services as possible, consider sharing personal information only with people you know. Recently we have become aware of “catfishing” or the use of “sock puppets” that are people developing fake online personas specifically to deceive, obtain information or manipulate people. If you expand your contacts beyond people you are sure you can trust, check the service’s settings to see if you can group your contacts and assign different levels of access based on your comfort level. Attackers may adopt different identities to try to convince users to add them as contacts, so try to confirm that contacts are who they claim to be before giving them access to your information.