Procedure
1078.1

SCHOOLCRAFT COLLEGE

18600 Haggerty Road, Livonia, Michigan 48152-2696

SOCIAL MEDIA GUIDELINES

The following principles apply to use of social media on behalf of the College, as well as personal use of social media when referencing the College:

1. Employees need to know and adhere to the College Workplace Conduct Procedure 4060.1, and other College policies and procedures, when using social media in reference to the College.

2. Employees should be aware of the effect their actions may have on their image, as well as the College's image. Employees are personally responsible for the content they publish on blogs, wikis or any other form of user-generated content. Employees should be mindful that what they publish will be public for a long time and they should take steps to protect their privacy and that of others.

3. Employees should be aware that the College may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to the College, its employees, students, or the community.

4. Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.

5. Employees may not use social media to harass, threaten, insult, defame or bully another person; or to violate any College policy; or to engage in any unlawful act, including but not limited to: gambling, identity theft or other types of fraud.

6. Employees should not make false claims or representations about College programs or services, nor speculate, spread gossip, rumors, or other unverified information.

7. Employees should not transmit chain letters, junk email, or bulk communications.

8. Employees should not insult, disparage, disrespect or defame the College or members of the College community.

9. Employees should not discuss legal issues or risks, or draw legal conclusions on pending legal or regulatory matters involving the College.

10. Employees should not publish, post or release any information that is considered confidential or not public, including but not limited to, information protected from disclosure by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Family Educational Rights and Privacy Act (FERPA). If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or their supervisor.

11. Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized College spokespersons. If employees encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.

12. Employees should get appropriate permission before referring to or posting images of current or former employees, students, vendors or suppliers.

13. Employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.

14. Employees should not allow social media use to interfere with employee’s responsibilities at the College.

15. The College’s computer systems are to be used for business purposes only. When using the College’s computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, College blogs and LinkedIn), but personal use of social media networks or personal blogging of online content is prohibited and could result in disciplinary action, up to and including termination.

16. Subject to applicable law, after-hours online activity that violates the College’s policies may subject an employee to disciplinary action, up to and including termination.

17. If employees publish content after-hours that involves work or subjects associated with the College, a disclaimer should be used, such as this: “The postings on this site are my own and may not represent the College’s positions, strategies or opinions.”

18. It is highly recommended that employees keep College-related social media accounts separate from personal accounts, if practical.

19. It is prohibited to use the College’s logo and trademarks on employees’ personal sites for any reason and especially not to promote any products, causes, or political parties or candidates.

20. The College encourages freedom of expression and recognizes the value of diverse opinions. However, page administrators have a responsibility to remove comments, images, or other material deemed inflammatory, vulgar, or otherwise inappropriate, especially when they appear to threaten the welfare or safety of the poster or others.

21. The College is aware that members of the College community may wish to express their personal ideas and opinions through private social media that are not administered by the College. Nevertheless, the College reserves the right, under circumstances it deems

appropriate and subject to applicable laws and regulations, to impose disciplinary measures, up to and including dismissal from the College or termination of employment, upon students, faculty, or staff who use private social media sites or communications resources in violation of this procedure or in ways that reflect poorly on the College or are deemed to interfere with the conduct of College business. In appropriate cases, such conduct may also be reported to law enforcement authorities.

22. Non-compliance with this policy may result in any or all of the following:

    a. Limitation or revocation of individual or unit rights to use or participate in College related social media;

    b. Removal of posts or social media accounts; or

    c. Corrective or disciplinary actions and sanctions.

23. Reporting Social Media Posts:

    If a post is deemed a potential threat to students, faculty, staff or any of the campus locations, it should be reported immediately to Campus Police at (734) 462-4424, with a follow up report submitted via SC Aware at www.schoolcraft.edu/scaware/sc-aware.

    If the content of a post is deemed to require personal counseling; especially, in a case where it could potentially elevate into an emergency situation, please immediately contact Student Relations at (734) 462-4429 and follow up by submitting a report via SC Aware at www.schoolcraft.edu/scaware/sc-aware.

24. Recommended Safety Tips for Social Media

    Social media platforms are great tools for connecting with friends, family members and working professionals. However, using social networking tools and sites seems to be in direct conflict with another important principle of using the Internet – protecting identities from identity theft. Participating in online social networking sites leaves a trail of personal information that can make stealing identities a lot easier.

    1. Be selective with friend requests.

        a. If the person is unknown, don’t accept the request, as it could possibly be a fake account.

        b. If a message is suspected to be fraudulent, use an alternate method to contact the sender to confirm authenticity; this includes invitations to join new social networks.

    2. Click links with caution.

        a. Look out for language or content that does not sound like something friends or family would post.

        b. Use caution when clicking links that are received in messages from friends or family on social websites.

c. Treat links in messages on these sites like links in email messages.

3. Choose social networks carefully; evaluate the site to be used and make sure the privacy policy is understood. Become familiar with the privacy policies and customize privacy settings to control who can view the content.
4. Assume that everything put on a social networking site is permanent. Even if the account can be deleted, anyone on the Internet can easily print photos or text or save images and videos to a computer.
5. Protect electronic devices by installing antivirus software. Also ensure that browsers, operating systems, and software are kept up to date.
6. Remember to log off when done using applications and devices.

Adopted—Cabinet
March 19, 2019