Oakland Community College Effective Date: 11-2013

Ownership/Source: Marketing Dept. Revised Date:

Approved by: Chancellor's Cabinet

Contents

Introduction

Social media is an umbrella term that defines the various activities that integrate technology, social interaction and content creation ("collaborative tools"). Social media uses the "wisdom of crowds" to connect information in a collaborative manner online. Through social media, individuals or collaborations of individuals engage with their audience, begin and join conversations, create web content, organize content, edit or comment on content, combine content, and share content.

Social Media Guidelines

Social Media Guidelines have been created to provide OCC employees, students, and contractors direction in using and/or creating social media. These guidelines are maintained by the Marketing & Communications Department.

Authorization to create and administer social media sites on behalf of OCC must be coordinated through the College Marketing & Communications Department. The Marketing & Communications Department is the official keeper of the OCC brand and must ensure all OCC social media sites are correctly branded both visually and with the right voice, and are managed by approved users (admins). It is appropriate to post to OCC authorized social media sites (see page 11) if posts are directly related to OCC business.

Social media sites have varying levels of privacy settings and terms of agreement. Agents posting on behalf of OCC must be aware of the social media site's privacy policy, terms of use, and community guidelines. Social media privacy settings change frequently, and it is each user's responsibility to stay up to date. Be aware no social media privacy option completely protects information from being shared beyond desired boundaries. **FERPA** and **HIPAA** privacy laws apply to posting or transmitting of confidential information to social media sites.

Posts on OCC official social media sites should protect the College voice by remaining professional. No individual department should construe its social media site as representing the College as a whole. Consider this when naming OCC official pages or sites, selecting a profile picture or icon, and selecting content to post. Names, profile images, and posts should all be clearly linked to the particular department or unit rather than to the institution as a whole. However, the department sites must be up to brand standards and appear cohesive with the official brand. The Marketing & Communications Department can assist and advise you with your social media planning.

Link back to OCC: Whenever possible, link back to the OCC website. Ideally, official OCC posts should be very brief; redirecting a visitor to content that resides within the OCC web environment. When linking to a news article about OCC, check first to see whether you can link to a release on the OCC webpage instead of an outside media source. If you have questions, contact the Manager of Multi-Media and Web Services at 248.232.4423.

EMPLOYEE GUIDANCE FOR PARTICIPATING IN SOCIAL NETWORKING

Employees should remember that students and the community might judge them and OCC by their posts. Employees should be honest and transparent about their identity and role at OCC. No single employee is permitted to act as an official voice of OCC. Maintain accuracy by verifying facts before posting information via social media. Exercise restraint and be fair and courteous with respect to the opinions of others. Do not use OCC-related social media to promote services, products or organizations that are unrelated to OCC or its business. OCC employees and students should use good judgment in connecting with others via social media sites. Employees, students, or contractors who act in a manner inconsistent with these guidelines may be subject to discipline up to and including discharge.

Employees will keep their personal social media sites separate from OCC social media. In personal posts, employees may identify themselves as an OCC faculty or staff member and post as it relates to their professional role at OCC.

GUIDELINES FOR ALL SOCIAL MEDIA SITES

- **Protect confidential information**: Do not post confidential information about OCC, students, employees, or alumni. Employees must know and understand the Social Media and **FERPA** guidelines. Employees who share confidential information do so at the risk of disciplinary action.

- **Respect copyright and fair use:** When posting, be mindful of the ***Copyright and Fair Use Guidelines for Educators Used by OCC.*** If you have questions or concerns, contact your campus copyright resource person.

- **Don't use OCC's logos for endorsements:** Do not use the OCC logo or any other College images on personal social media sites. Do not use OCC's name to promote a product, cause, or political party or candidate.

- **Respect College time and property:** College computers and time on the job are reserved for College-related business as approved by supervisors and in accordance with the OCC **Technology Appropriate Use Regulations (TAUR).**

BEST PRACTICES

- **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 it may reflect both on the poster and the College. Search engines can turn up posts years after they are created, and comments can be forwarded or copied. Archival systems save information even if you delete a post. If you wouldn't say it at a conference or to a member of the media, consider whether you should post it

  online. Be mindful of spelling and grammar in social media posts—if space is limited (i.e., on Twitter,

Tweets are limited to 140 characters), be sure to use well-known abbreviations and punctuations that are not confusing. If you are unsure about posting something or responding to a comment, ask your supervisor for input or contact the College Manager of Multi-Media and Web Services at 248.232.4423.

- **Legal matters and crisis situation topics:** Never comment on legal matters, including past or present litigation. Also, refrain from posting on crisis situation topics.

- **Be respectful:** You are more likely to achieve your goals or sway others to your beliefs if you are constructive and respectful while discussing a bad experience or disagreeing with a concept or person. As an OCC employee, you understand the College's commitment to respect for the dignity of others and to the civil and thoughtful discussion of opposing ideas. Some online communities can be volatile, tempting users to behave in ways they otherwise wouldn't. Your reputation and OCC's are best served when you remain above the fray. Nevertheless, if you decide to post criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating or that might constitute harassment or bullying. Examples of such conduct could include posts meant to intentionally harm someone's reputation or posts that would create a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or policy.

- **Don't be a mole:** Never pretend to be someone else. Tracking tools enable supposedly anonymous posts to be traced back to their authors.

- **Strive for accuracy:** Make sure you have all the facts before you post. It's better to verify information with a source first than to have to post a correction or retraction later. Cite and link to your sources whenever possible. This is especially important if posting on behalf of the College in any capacity. Review content for grammatical and spelling errors. Also reference the College Writing Standards.

- **Remember your audience:** Be aware that a presence in the social media world is or easily can be made available to the public at large. This includes prospective students, current students, community and peers. Consider this before publishing to ensure the post will not alienate or harm any of these groups.

- **Be transparent:** Your honesty—or dishonesty—will be quickly noticed in the social media environment. If you are commenting about OCC, use your real name, identify that you work for OCC, and be clear about your role. If you have a vested interest in something you are discussing, be the first to point it out. Transparency is about your identity and relationship to OCC.

- **On personal sites:** Identify your views as your own. If you identify yourself as an OCC faculty or staff member, it should be clear the views expressed are your own and not necessarily those of the institution.

- **Write what you know:** Make sure you write and post about your areas of expertise, especially as related to OCC and your department. If you publish to a website outside OCC, please use a disclaimer something like this: "The postings on this site are my own and don't necessarily represent OCC's positions, strategies, or opinions."

- **Perception is reality:** In online social networks, the lines between public and private, personal and professional are not clear. Just by identifying yourself as an OCC employee, you may create perceptions

about your expertise and about OCC by our students and community, as well as your own perceptions about you by your colleagues. Be sure all content on OCC sites is consistent with your work and with OCC's values and professional standards.

- **It's a conversation:** Talk to your readers as you would talk to real people in professional situations. Consider content that's open-ended and invites response. Encourage comments.

- **Are you adding value:** The best way to get your comments read is to write things people will value. Social communication from OCC should help our students, community and co-workers. It should be helpful and informative. If it helps students or the community - then it's adding value.

- **Your responsibility:** What you write is ultimately your responsibility. Participation in social networking on behalf of OCC is not a right but an opportunity, so please treat it seriously and with respect. If you want to participate on behalf of OCC, it is important you read and understand all of the Social Media Guidelines.

- **Did you screw up:** If you make a mistake, admit it. Be upfront and quick with your correction. If you're posting a comment and you choose to modify an earlier post—just make it clear you have done so.

- **If it gives you pause, pause:** If you're about to publish something that makes you even the slightest bit uncomfortable, don't shrug it off and hit "send." Take a minute to review these guidelines and try to figure out what's bothering you, then fix it. If you're still unsure, you might want to discuss it with your supervisor. Ultimately, what you publish is yours—as is the responsibility.

- **Photography:** Photographs posted on social media sites can be easily appropriated by visitors. Consider adding a watermark (faded image of the logo over the photo) and/or posting images at 72 dpi and approximately 800x600 resolutions to protect your intellectual property. Images at that size are sufficient for viewing on the Web, but not suitable for printing.

- **Stay engaged and active:** If another user engages with your account (i.e., writing on your Facebook wall), be sure to engage them in conversation. If they ask a question, answer it. If they share a photo, thank them for it. This will encourage others to join the conversation and view the account as a reputable place to get information and answers.

- **Encourage cross-promotion**: All OCC social media sites should be working together to help promote news, information, events, etc. to the OCC community. Encourage different social media sites to share information from other sites to their own (Ex: The English Department can

  share a Facebook post from the OCC-official page). This will expand the reach of the information to more social media users.

Social Media Roles and Responsibilities Section

- The IT Department is responsible for the technology and technical support for social media users. This includes:

- Providing analytical software for tracking social media use
- Updating web links to social networks from the OCC website(s)

- The Marketing & Communications/Multi-Media and Web Services team is responsible for supporting the use of OCC social media as a communication tool. This includes:
  - Creating content for the official OCC social media channels
  - Reviewing requests for social media sites and approving as appropriate
  - Reviewing requests for official OCC social media posts and posting as appropriate
  - Maintaining an inventory of all official OCC social media sites
  - Monitoring and evaluating official OCC social media sites
  - Tracking and analysis of the official College's social media channels using analytic software and other monitoring tools
  - Removing threatening posts on official OCC social media (and referring them to Public Safety) or those including inappropriate language
  - Maintaining College identity standards on official OCC social media channels

- OCC social media sites are not public forums and may not be used to advance the personal causes or issues of a user or denigrate the College, other persons, or groups of people. Threats of violence, profanity, and obscene statements or images are prohibited, and intellectual property rights must be respected at all times. Postings that violate any one or more of these restrictions will be removed by the College, and the person who posted them will be denied further access to OCC social media sites.

- All representation of official OCC information, services, media, logo, graphics, and other materials on social media sites are considered an extension of the College's information networks and are governed by the standards and guidelines presented herein. They are further governed by OCC Board of Trustees policies and the Technology Appropriate Use Regulations.

- Departments that have a social media page or would like to start one should contact the Manager of Multi-Media and Web Services at 248.232.4423 or e-mail mrkerste@oaklandcc.edu to ensure all institutional social media sites coordinate with other OCC sites and their content. All College pages must have a full-time appointed employee who is identified as being responsible for content.

  Because OCC has no control over social media sites created in the internet community at large, official OCC sites will be recognizable by their name and by the use of the official OCC logo. All OCC Social Media Groups created by the College Marketing & Communications Department shall be named using the following format: "Oakland Community College – *Identifying Department Name.*"

  Example: Oakland Community College – English Department

- Department directors must approve the creation of all OCC official social media tools before they are brought to the Manager of Multi-Media and Web Services for approval. The Manager of Multi-Media and Web Services has final approval of all social media sites to ensure proper branding and alignment with College goals. Employees who use social media on behalf of their department or the College are acting as official representatives of Oakland Community College. Users of social media must realize their postings will be permanently available on the internet and can be reproduced by other media.

- All official OCC or departmental social media sites, whether created by an individual or department, are the property of OCC. All information on OCC sites, including login and password information, and the names of authorized users, must be provided to the Marketing & Communications Department. Passwords for OCC sites cannot be changed without notifying and updating the Marketing & Communications Department.

- The content of each authorized social media outlet shall be maintained by and is the sole responsibility of the department producing and using the site or service. All individuals participating in social media on behalf of OCC must be trained in the guidelines documented herein.

- Social media users are responsible for complying with applicable federal, state and local laws, regulations and policies. This includes adherence to established laws and policies regarding copyright, records retention, and the Freedom of Information Act (FOIA), First Amendment, and privacy laws, including CIPA and Family Educational Rights and Privacy Act (**FERPA**).

Overview of Social Media Security Threats

Oakland Community College has a requirement to protect its information assets and to safeguard its students and employees. The use of social media for College services and interactions is growing rapidly, supported by the College administration and demands from the public. This situation presents both opportunity and risk.

Information systems are susceptible to targeted attacks by individuals using technology to gain personal information or to cause harm. In April 2009, the Federal Bureau of Investigation released a Headline Alert specifically citing social networking sites as a mechanism for attackers to gather information on their targets by harvesting information from publically-accessible networks and using the information to launch an attack. In order to defend against these rapidly evolving attacks, people must learn about the methods used by potential attackers.

Some of the more common threats are detailed below.

- **Spear Phishing**

  Spear phishing is an attack targeting a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans or current issues. This information is often gathered by looking up the target on social media sites.

- **Social Engineering**

  Social engineering is the exploitation of the human element of trust. Social engineering attacks begin with collecting information about the attacker's target. This information resides on social media sites in various ways, including resumes, home addresses, phone numbers, employment information, work locations, family members, education, photos, and private information.

Often an attacker uses the information gathered from social media sites to build a trust relationship with the target. Once the victim trusts the attacker, the attacker can collect more information about the user or use their relationship to expand their influence. The result can be the attacker gathering enough personal information on the target to potentially steal someone's identity, gain access to banking information, etc.

- **Web Application Attacks**

  Web applications are dynamic web pages that use scripting and other dynamic code to provide additional functionality to the user. They can be developed and used by attackers on social media sites. For instance, techniques include using custom Facebook applications to target users. Facebook applications are written by third-party developers and often have minimal security controls.

  These applications are used to grant the malicious application access to the user's personal information contained within the social media site account, as well as access to post things on behalf of the user. While a hijacked personal social media account may be annoying and personally costly and embarrassing, a hijacked account from an official College site or a known College employee may have more serious implications. Unofficial posts, tweets or messages may be seen by the public as official messages, or may be used to spread malware by encouraging users to click links or download unwanted applications.

Protective Measures

Consider the following security measures when engaging in social media:

- Make sure your computer or internet capable device is protected before using the internet in any fashion and especially when visiting social media sites. Make sure you have firewall and anti-virus software that is kept **up to date**. Keep your operating system up to date as well.

- Do not assume you are in a trusted environment just because you are on someone's page you know. It is prudent to use caution when navigating pages and clicking links or photos. Links, images or other content contained in those pages can contain malicious code.

- Be cautious in how much personal information you provide on the internet and especially on social media sites. The more information you post the easier it is for an attacker.

- Use common sense when communicating with users you DO know. Always validate electronic requests when it relates to money, personal identity, account numbers and/or password information. The communications could be from someone who has hijacked the account of the person you know with the intent on scamming others.

- Use common sense when communicating with users you DON'T know. Be cautious about whom you allow to contact you or how much and what type of information you share with strangers online.

- Understand what information is collected and shared. Pay attention to the policies and terms of the sites and social media platforms accessed; they may be sharing your email address or other details with other companies.

- Do not download or use applications associated with social media sites, such as Hoot Suite, on OCC hardware (computers, smartphones) unless approved by the Marketing & Communications Department or Multi-Media and Web Services Manager.

- Do not click links or open email messages sent through private social media sites unless you are certain they are from a trusted source. Be wary of unusual "subject" fields in messages, as these are often a sign that an attacker has taken over the account where the message originated from.

Electronic Records Management

- Record retention of social media posts, comments, and private messages is important. Posts, comments, and messages are considered electronic communications as detailed in OCC policy, and are to be retained according to the retention standards established by the College.

- The following is to be applied in regards to record retention.
    - If the posts are made or received in connection with the transaction of OCC public business (such as providing advice or receiving comments about the department, its programs, core business, etc.), then they are public records for the purposes of records retention and need to be retained for their minimum retention periods.
    - Record retention standards for posts shall coincide with the standards used for both electronic and non-electronic communications sent within the College's jurisdiction.
    - If something needs to be deleted, a copy shall be retained and removal reasons listed, along with the date of removal.

Disclaimers

The following should be used on all OCC-related social media sites, as applicable.

User-generated Content and Disclaimer

Oakland Community College accepts no responsibility or liability for any data, text, software, music, sound, photographs, images, videos, messages, or any other materials whatsoever ("Content") generated by users ("the Users") and publicly posted on this page.

Disclaimer for content on linked sites

The only "Official" social media sites include the:

- OCC Facebook page: Oakland Community College (official),
- OCC Twitter page: OCCollege,
- OCC YouTube channel: OCCollegeOfficial YouTube,
- OCC news blog: occblognnews,
- OCC Alumni LinkedIn page: Oakland Community College Alumni (official),
- OCC Fire/EMS Facebook page: Oakland Community College Fire/EMS Training and the
- OCC Economic and Workforce Facebook page: Oakland Community College – Economic and Workforce.

Oakland Community College accepts no liability or responsibility for the contents of any other target site linked from this page.

Terms of Use
By posting content on this page you agree to comply with the terms and conditions of this site (e.g. Facebook) and Oakland Community College Social Media Guidelines. In particular, you represent, warrant, and agree that no content submitted, posted, transmitted, or shared by you will infringe upon the rights of any third party including, but not limited to, copyright, trademark, privacy; or contain defamatory or discriminatory or otherwise unlawful material.

Oakland Community College reserves the right to alter, delete or remove (without notice) the content and remove or ban users at its absolute discretion for any reason whatsoever.

VIOLATION OF THESE GUIDELINES CONSTITUTES GROUNDS FOR DISCIPLINE AS AUTHORIZED BY BOARD POLICY 3.8.2.

Copyright
The content on this page is subject to copyright laws. Unless you own the rights in the content, you may not reproduce, adapt, or communicate without the written permission of the copyright owner nor use the content for commercial purposes.

Reporting Abuse
Most platforms encourage all users to report abusive content. To make a report, follow each platform's instructions.

Social Media Guidelines for Students

Why?

Social media tools have become widely accessible and are often used in classroom (real or virtual) activities. It is important to be aware of how the content you post can affect you and your peers. Additionally, remember what you post can reach audiences far beyond the classroom for an unlimited length of time. You need to also be mindful that social media usage has some common risks and should be used very carefully.

Dos

1. Be aware of what you post online. What you contribute leaves a digital footprint for all to see and can be permanent.
2. Be respectful. Even if you are expressing a difference of opinion, be fair and courteous. Keep it constructive and not hurtful. If you do decide to post complaints or criticism, avoid using comments, photographs, video or audio that could be viewed as malicious, obscene, threatening, bullying, harassing or intimidating. What is inappropriate in the classroom is inappropriate online.
3. Be aware that certain "non-verbal" cues (such as tone of voice) get lost when translated online.
4. Review links before sharing them online to make sure the material is appropriate for the classroom.
5. Get permission to repost copyrighted material. Although easily accessible, reposting pictures or content you did not create on the internet may violate copyright laws.

Don'ts

1. Don't post anything on the internet you would not want your instructors or employers (current or future) to see. Anything you post, even if you label it "private," may be accessible or visible to others.
2. Don't post combative responses to other students' or instructors' comments.
3. Don't abandon inhibitions you would have in normal, face-to-face communication. If you wouldn't say it in person, don't say it online.
4. Don't misrepresent yourself by using anyone else's identity.