10 Tips for Social Workers using Social Media and Technology

1. **Do not "friend" clients**
   Social workers need to write a policy that prohibits connecting with clients on social networking and media sites to avoid raising boundary issues. It includes, but not limited to, Facebook, LinkedIn, Instagram, and Twitter. Clients are not friends, and social workers need not collect followers. The Kentucky Code of Ethical Code and the NASW Code of Ethics both speak to the matters of boundaries, multiple relationships, and conflicts of interest. This responsibility does not change with the use of social media.
2. **Do not blog, post or make comments about clients, colleagues or work matters**
   Social workers should be keenly aware of the implications of connecting with colleagues, even for informal consultations in a private group. Social workers who post comments related to their employment must be conscientious or just avoid posting. Social workers are held professionally accountable for their own posts and can be responsible for everyone in their network. Unknowing and untold harm can be done when information "leaks" from social media or other accounts into the public forum. This can be about clients, colleagues, or co-workers. The information may be confidential or just not for public consumption. Just keep in mind that posts and comments are read by your clients, employers, or colleagues and maybe scrutinized through many lenses like Confidentiality, Unethical Conduct of Colleagues, Commitment to Employers, and Private Conduct, to name a few. Standards apply online just as they do in the work environment.
3. **Manage the privacy and location settings on your social media accounts**
   Do you know what comes up when people search your name on the Internet? Try it! What personal information do your clients and colleagues have access to? Even though social workers may have the most secure privacy settings, social media sites cannot and do not guarantee complete privacy. Furthermore, social media security and privacy are often compromised by updated policies that require action to maintain confidentiality, e.g., who can see your profile information, visibility of what you or your friends share or post on sites, etc. It depends upon you to stay abreast of your online profile and manage what you post.
4. **Do not search your clients on the web**
   This may sound odd, given the above point. However, searching for clients without their permission may lead to bias and unnecessary conflict with clients. Search clients when there is a defensible professional need to do so, such as protecting life and property. Before deciding to search for a client, social workers should:
   - Discern whether the search is clinically indicated and governed by standards of practice as opposed to satisfying personal curiosity
   - Be aware of the impact that the results might have on the social worker and client relationship
   - Consider the need to include searching in the informed consent and any social media policy
   - Consider how to verify any information gleaned from social media or other web locations.
5. **Implement a social media and technology policy, review and update**
   Having **a well-**written statement about social media and technology can mitigate a lot of unnecessary headaches. Be very clear about your policy at the beginning of any client or collegial engagement. Be consistent in its application; exceptions can

damage your credibility big time. This also applies to individual practitioners, agencies, and other employers. If you already have a social media policy, review and update it annually at the minimum. You may want to have clients sign that they understand your policy.

6. **Help clients become aware of how their use of social media, apps, and other technology may compromise their confidentiality**

   It is essential to discuss with clients as soon as possible and as often as necessary after that, the importance of discretion with their use of social media and technology, i.e., texting and check-ins. Let them know that if they engage in this activity that you are not responsible for their disclosures. Again, the importance of a written policy. Here are some points to share with your clients:

   - Clients who activate location-based services on social media and other sites may be unknowingly divulging their whereabouts, and that they are in your office for a therapy session.
   - Web sites that allow users to rate their practitioners may also compromise the client's confidentiality.
   - Following and friending their therapist may compromise the client's confidentiality

7. **Implement privacy and privacy measures for electronic communications and records, e.g., encryption and password-protected access, especially if you are a covered entity by HIPAA**

   Social workers who choose to communicate electronically with clients by using e-mail, text messaging, or video conferencing must be aware of the risks involved. The NASW Code of Ethics (1.07 (m)) states, " Social workers should take reasonable steps to protect the confidentiality of electronic communications, including information provided to clients or third parties. Social workers should use applicable safeguards (such as encryption, firewalls, and passwords) when using electronic communications such as e-mail, online posts, online chat sessions, mobile communication, and text messages."

8. **Be very careful about allowing testimonials from current or former clients**

   This tip may sound odd; however, it is an activity fraught with conflicts of interests, boundaries, and dual relationship issues. The power differential between the social worker and the client can always be a factor in this arena. Not only seeking testimonials but also trying to respond to a negative online review is just as dangerous.

9. **Be cautious in using electronic payment systems.**

   The use of PayPal, Venmo, ApplePay, etc. may not be in the interest of clients or the social worker. The social worker's name may appear on bank transactions and statements and might be a violation of confidentiality. It does not mean that these services cannot be used. It means that the social worker and the client need to have a clear understanding of how the preferred method of payment works to avoid unknowingly making a violation.

10. **Be cautious of the use of cell phones and voice over IP (Internet)**

    Cell phones are fantastic devices and can be an invaluable tool for social workers. However, using FaceTime or Skype may violate confidentiality as the display of the caller's face can be visible to others nearby. The same goes for when the social worker calls the client. Standard texting is not secure, so this is an added concern as clients often want to use this method to make or change appointments or meeting places. The use of unsecured texting must be agreed to in writing between the social worker and the client. Most phone services now use the Internet to transmit calls. If the social worker is under strict confidentiality rules, think HIPAA, they may

need to have a business associate agreement with their phone carrier for VOIP.

The NASW Code of Ethics was revised in 2017 and had a lot to say about the use of technology, including search. This is the new standard care even when social workers are not members of NASW.

In addition, standard 2.06, Standards for Technology in Social Work Practice, states, "Social workers who use technology to provide services shall obtain and maintain the knowledge and skills required to do so in a safe, competent, and ethical manner." The NASW Code of Ethics (1.04(d)) extends the concept of competence to include the ability to use technology competently. Social workers who use technology need to understand the possibility of communication challenges and how to address these challenges from dropped calls to power failures. Social workers are now responsible for becoming proficient in the technological skills and tools required for competent and ethical practice. They are also responsible for seeking appropriate training and consultation to stay current with emerging technologies.

The ethical standards that apply to in-person communication and documentation also apply when communicating electronically. Also, it should be noted that it is not uncommon for e-mail, texting, and other electronic communications to be included in subpoenas and other legal and professional review matters. Social workers who converse with clients electronically should consider establishing an authorization process to help lessen some of the risks involved.

Resources

- NASW Code of Ethics revised 2017
- NASW & ASWB & CSWE & CSWA Standards for Technology in Social Work Practice revised 2017
- Eye on Ethics: Developing a social media ethics policy - Social Work Today, July 1, 2001
- It's better to be informed about tech tools - NASW News, June 2011
- Professional Ethics and Social Networking - NASW Specialty Practice Sections course
- The Interface of Ethics and Technology by Frederic Reamer, Ph.D. PESI 2014