Guideline: Social media and the nursing profession: a guide to maintain professionalism online for nurses and
nursing students - 2019

Acknowledgements

Contents

Purpose and Introduction

The New Zealand Nurses Organisation, Tōpūtanga Tapuhi Kaitiaki o Aotearoa (NZNO), Nurse Educators in the Tertiary Sector (NETS) and the NZNO National Student Unit and Te Rūnanga Tauira (NSU/TRT) are committed to upholding the professional standards of nursing. The purpose of these practical guidelines is to help nurses and nursing students enjoy online activity while maintaining professional standards in Aotearoa New Zealand.

Nurses are expected to maintain the highest professional standards at all times. Professional standards are set by nursing's professional bodies and the Nursing Council of New Zealand (NCNZ), based on the expectations of the community and peers. The Nursing Council provides guidelines on professional boundaries and social media and electronic communication, publishes a code of conduct, and sets competencies for practice (NCNZ, 2009; NCNZ, 2012a; NCNZ 2012b). Professional standards are taught and assessed from the first year of nursing education and nurses are expected to maintain these standards throughout their careers (NCNZ, 2010). NZNO publishes standards of practice and a code of ethics (NZNO, 2012; NZNO, 2010).

Social media use has increased rapidly in recent years (Adhesion, 2018). Social media consists of the internet or web-based technologies that allow people to connect, communicate and interact in real time to share and exchange information. This may include using Facebook, Twitter, YouTube, Snapchat, Instagram, blogs, forums, dating "apps" and personal websites. The key element of social media that differentiates it from traditional internet use is the active nature of the dialogue, enabling user-generated content and images to be communicated instantly.

Nurses and nursing students are increasingly participating in online social media but evidence is emerging from studies, legal cases and media reports that the use of social networking can pose risks for health professionals. Inappropriate online behaviour can potentially damage personal integrity, nurse-patient/client relationships, nurse-colleague relationships, current and future employment opportunities.

General Principles

As a rule, the following guiding principles adapted from the American National Council of State Boards of Nursing (NCSBN 2018) should help keep you safe as you use social media:

- You have an ethical and legal obligation to maintain patient/client privacy and confidentiality at all times.
- Never transmit by way of electronic media any patient/client-related image or any information that may either actually, or potentially violate patient/client rights to confidentiality or privacy, or otherwise degrade or embarrass the patient/client.
- Do not access, share, post or otherwise disseminate any information, including images, about a patient/client, or information gained in the nurse-patient/client relationship, with anyone, unless there is a patient/client care related need to disclose the information, or other legal obligation to do so.
- Do not identify patient/client by name or post or publish information that may lead to identification of a patient/client. Limiting access to postings through privacy settings is not sufficient to ensure privacy.
- Never refer to patient/client in a disparaging manner, even if the patient/client is not identified.
- Do not take photos or videos of patient/client on personal devices, including cell phones. Follow employer, university, polytechnic or wānanga policies for taking photographs or video of patient/client for treatment or other legitimate purposes, using employer, university, polytechnic or wānanga-provided devices.
- Maintain professional boundaries in the use of electronic media. As with face to face relationships, the nurse has an obligation to establish, communicate and enforce professional boundaries with patient/client in the online environment. Use caution when having online social contact with patient/client or former patient/client and/or their family or whānau members. It may be prudent to avoid such contact.
- Avoid patient/client-targeted Googling
- Consult employer, university, polytechnic or wānanga policies, or an appropriate leader within the organisation, for guidance regarding work or student-related postings.
- Promptly report any breach of confidentiality or privacy.
- Be aware of, and comply with employer, university, polytechnic or wānanga policies regarding use of organisation-owned computers, cameras and other electronic devices, and use of personal devices in the workplace or school.
- Do not make disparaging comments about employers, co-workers, teachers or fellow students. Never make threatening, harassing, profane, obscene, sexually explicit, racially derogatory, homophobic or other offensive comments.
- Do not post content or otherwise speak on behalf of the employer, university, polytechnic or wānanga, unless authorised to do so, and follow all applicable policies.

Glossary

- **Third party apps**: Applications that are provided by vendors other than the manufacturer, e.g. iPhone have a camera app however, other camera apps are often downloaded as they provide additional services.
- **Social media**: Social media is any platform that allows users to share content and engage in social networking. Social media platforms that are currently heavily utilised include Facebook, Instagram, Twitter and Snapchat.
- **Privacy settings**: Privacy settings are controls available on many social networking platforms that allow users to limit who can access their profile and the information visitors can see.
- **Data harvesting**: The collection of personal information from social media platforms. Once collected, data can be used for advertising, identity theft, mapping user trends and hacking.
- **Big data:** Refers to analysis of large sets of data often gained through data harvesting. This data is used to create detailed maps of users' interactions online and is often used by businesses to create marketing strategies. A recent example of 'big data' is the 2018 Cambridge Analytica scandal, in which data was collected from over 87 million Facebook users and was used by select politicians to advertise to voters.
- **Patient/client-targeted Googling (PTG):** the use of social media or publicly available search engines by health professionals, perhaps in an emergency, to find information about a patient/client online.

Using social media constructively...

While using social media poses particular challenges for nurses, social media can also provide opportunities for connecting nurses with others, as well as enhancing and supporting nursing practice. It is essential nurses who use social media follow the guidelines provided and are aware of the pitfalls of social media before they start using it. This should not limit the potential of social media as a useful tool for the nursing profession.

Examples:
Discussion forums (either through Facebook or other platforms) provide an opportunity to reflect and discuss issues relevant to nursing.

Most nursing students participate on the class Facebook page and the NSU and TRT Committee uses Facebook as its main method of communication.

NZNO uses Facebook to keep members informed about campaigns and events.

The New Zealand College of Primary Health Care Nurses and the Child and Youth Nurses use Facebook to distribute consultation requests, advertise events and promote their journal which is then shared via social media with a wider audience.

A website for school nurses in Aotearoa was set up early in 2018 and includes a blog for school nurses to connect with colleagues for guidance.

Example:
Clinical applications utilising Social Media are also growing. These range from hospitals 'tweeting' progress in surgery to family members and information sharing and clinical consultation

---

Nurses using public platforms such as social media to express their opinion (which all people have the legal right to do – see the Employment Relations Act 2000 clause 14) must make a professional judgement about any potential risk to their own, their colleagues', and/or patient/client privacy and confidentiality (ERA 2000, clause 17), and their professional accountability.

Example: Erica is a practice nurse in a busy general practice and urgent care clinic. She follows the Twitter account @WeNurses to seek out quality improvement ideas in the online chat that could be applied in her workplace.

Be careful about what you say and how you say it

Confidentiality:

Example:

You are working in a rural hospital in a small, well-connected community and make a comment on a social networking site about an adverse outcome for a patient/client.

A cousin of that patient/client searches the internet for the hospital's name to find its contact phone number. In the search results, the cousin is presented with your posting about the adverse outcome for the patient/client and recognises the circumstances as those of her family or whānau member.

Nurses have an ethical and legal responsibility to maintain patient/client confidentiality. This still applies when using any form of online tool, regardless of whether the communication is with other nurses, a specific group of people (e.g. 'friends' on social networking sites), or the public (e.g. a blog). The anonymity potentially afforded online is no excuse for breaching confidentiality.

Before putting or accessing patient/client information online, think about why you are doing it. You should inform the patient/client and gain their express consent, and acknowledge the consent has been obtained in any online posts. If you feel it is appropriate to discuss a patient/client case e.g. to further that patient's/client's care or the care of future patients/clients who present with a similar condition – care must be taken to ensure the patient/client de-identified. Using a pseudonym is not always enough; you might have to change case information or delay the discussion. The ability to access and index online information means that, although a single posting on a social networking website may be sufficiently de-identified in its own right, this may be compromised by other postings on the same website, which are just a mouse click away.

Similarly, searching for information about a patient online (patient-targeted googling or PTG), perhaps in an emergency, can breach patient confidentiality. A recent research project with final-year medical students (Chester et al 2017) found a low incidence of PTG, while use of social media was high with many participants in the 'frequent user' category. The frequent users were much more likely to have googled patients. The Medical Council of New Zealand (MCNZ) offers the following caution about the practice of PTG:

"You must exercise restraint in using social media to seek out information about your patients. Patients have expectations of privacy and may choose not to disclose certain information to you in a clinical setting—even when that information is openly accessible online. If you consider that it is medically necessary to view patients' websites or online profiles, seek their permission before accessing those sites. You should also confirm the accuracy and relevance of online information with the patient before using it to inform your clinical decision-making or entering it into the patient record" (MCNZ, 2016).

In maintaining confidentiality, you must ensure any patient/client or situation cannot be identified by the sum of information available online. The practice of 'data harvesting' increases the risk your carefully anonymised post can be linked to other information online that then makes the patient/client or the situation identifiable.

Some of the examples used in this guideline are based on a number of prominent cases involving nurses or nursing students who have breached patient/client confidentiality through online postings. Moreover, breaching confidentiality erodes the public's trust in the nursing profession, impairing its ability to care for patients/clients effectively. Breaching patient/client confidentiality can result in complaints to the Nursing Council (with potential disciplinary action, including loss of registration), involvement of the Privacy Commissioner, or even legal action (including civil claims for damages) https://www.privacy.org.nz/.

Buppert, in her 2018 Medscape blog makes four recommendations:
- maintain professional boundaries
- protect professional reputations - yours and others
- don't breach privacy or the requirements of the law
- take care not to establish a care relationship by responding to questions or comments online
  (Retrieved from https://www.medscape.com/viewarticle/892498)

Defamation:

Example:

You are a newly-graduated nurse on your first job in a large city hospital. You have been working for about six months and are an avid Facebook user. A friend sends you a link to a post made by a nursing colleague from the same unit you work in that accuses you of being incompetent and a bully. How can/should you respond to 'defend' yourself?

Example:

A group of nursing students used the Facebook page they had set up to support their learning, to discuss the marking of a recent assignment. One of the students made a 'flippant' comment that she thought the lecturer who had marked her assignment must have been drunk while doing so. The marking lecturer and the tertiary institution were clearly able to be identified. The situation was brought to the lecturer's attention by a colleague. The lecturer felt particularly compromised by the suggestion that she was drunk because she does not consume alcohol at all. She was also concerned because the organisation in which she was employed was identified and she did not feel able to refute the claim that she had been drunk while marking. The lecturer chose not to take the matter further because she feared the repercussions from her employer and students.

Defamatory statements:

● are published to a third person or group of people;
● identify (or are about) a patient/client/colleague/person ('subject'); and
● damage the reputation of the subject.

Defamation cases may be brought in a court of law against a nurse, and are civil claims, in which substantial monetary compensation can be awarded. The NZNO *Standards of Nursing Practice* (2012) specify nurses are responsible for entering into, and maintaining professional relationships with colleagues and employers. Be mindful of comments made about colleagues (nursing or otherwise), employers, and large organisations.

Keep your friends close and others … not so close

Nurse-patient/client boundaries:

> **Example:**
>
> You get a friend request on social networking site from someone whose name sounds very familiar, but they have a photo of a dog as their profile picture. You accept the request. After looking through their profile page, you realise that it is actually one of your previous patients/clients. The patient/client sends you a message to let you know that they cannot make their next clinic appointment, but would like some information about how to care for their plaster cast. The patient/client also throws in a cheeky comment about some photos they saw of you wearing a bikini at the beach.

Boundary violations can occur very easily online, and serious indiscretions may result in disciplinary action against the nurse. A power imbalance exists between nurses and patient/client, and the maintenance of clear professional boundaries protects patient/client from exploitation and nurses from professional misconduct. Nurses who allow clients to access their entire 'profile' (or similar), thereby introducing them to details about their personal lives well beyond what would normally occur as part of the usual therapeutic relationship, may violate professional boundaries.

In general, it is wise to avoid online relationships with current or former patients/clients. In 2008, a nurse who started a sexual relationship with a former patient/client after contacting her on Facebook was removed from the United Kingdom Register of Nurses (Nursing Standard, 2010). If a patient/client or former patient/client does request you as a friend on a social networking site, a polite message informing them that it is your policy not to establish online friendships with patients/clients is appropriate. Ignoring a Facebook friendship request is also an acceptable approach. It allows you to ignore the request without the person being informed, avoiding potential offence. Another mechanism used by some health professionals, is to create an online profile that is maintained as their professional page only, or to join a professional social networking site such as LinkedIn. Patients/clients can become friends or fans of this professional page, which only provides information relevant to the professional practice of nursing. It is also possible to pay companies to manage social networking profiles.

In some communities where, despite best intentions, a nurse may have a pre-existing relationship (including via social media) with someone who subsequently becomes a patient. A conversation with the patient about professional boundaries and how they apply while there is a professional relationship may be appropriate.

Other boundaries:

Other professional relationships may also become problematic on social networking sites. Think very carefully before allowing others (including employers and colleagues) to access personal information.

Colleagues' online conduct:

Inevitably, many people choose to interact with colleagues via social media. While you need to be aware of what they see you doing, you may also notice colleagues posting information online or behaving inappropriately. Looking after colleagues is an integral element of professional conduct, so if you feel a friend or workmate has posted information online that could be damaging for them, consider letting them know in a discreet way (such as a personal email, text message, or phone call).

Consider the destiny of your data

Extent of access to your information:

Many people are unaware of the easy accessibility and durability of their online information. Even if using the most stringent privacy settings, information on social networking sites may still be widely available, including to various companies and search engines. Deleting information is not sure-fire protection – social networking sites retain copies of information including private messages even after content has been deleted and can be retrieved later. If there is something you really do not want some people to know about you, avoid putting it online at all - even private messages can be accessed by hackers or third party applications. It is much harder to prevent other people posting information about you online (e.g. photos, videos). However, you can report inappropriate content to site administrators and request its removal.

The 10 principles for online/digital behaviour

Harmful Digital Communications Act 2015, s 6
The Harmful Digital Communications Act sets out 10 principles that apply to texts, emails and online posts – what the Act calls "digital communications".

NetSafe, as the new cyberbullying complaints agency, is supposed to take these principles into account when considering a complaint. If complaining to NetSafe doesn't solve the problem and you decide to take your complaint to the district court, the judge will also have to take these principles into account.

The new principles say that "digital communications" sent to you or are about you shouldn't do any of the following things:

- give out sensitive personal information about you
- be threatening, intimidating or menacing
- be grossly offensive, as judged by any reasonable person in your position
- be indecent or obscene
- be used to harass you
- make false claims about you
- contain information or material that you had given to someone in confidence
- encourage other people to send you a message for the purpose of causing you harm
- encourage you to kill yourself
- put you down ("denigrate" you) on the basis of your colour, race, ethnic or national origins, religion, gender, sexual orientation or disability.

(Ministry of Justice, 2015)

The **Harmful Digital Communications Act 2015** has set up special processes you can use if you're being harassed or bullied through texts, emails, websites, apps or social media posts. The aim is to provide a relatively quick and easy way for harm to be reduced, including by getting harmful posts or messages taken down or disabled, while at the same time giving people appropriate room for freedom of expression.

Harmful Digital Communications (Appointment of Approved Agency) Order 2016
One of the new features introduced by this Act is a special complaints and mediation agency. NetSafe, the internet safety organisation, has been appointed to play this role.

If going to NetSafe doesn't fix the problem, you can apply to the district court. The judge can do things like order the harmful post to be taken down, or order the person responsible to publish a correction or an apology.

The Act also establishes a number of specific principles to guide online/digital behaviour (see below). NetSafe and judges have to take these principles into account when they're dealing with claims that someone has been cyberbullied.
(Ministry of Justice, 2015)

Employee and student background checks

Recruiters are increasingly screening potential employees online. Employer surveys have found between one-fifth and two-thirds of employers conduct internet searches, including of social networking sites, and some have turned down applicants as a result of their searches (Brown & Vaughn, 2011).

Be conscious of your online image. While the employers, universities, polytechnics or wānanga you are applying to may find information about you online that could be advantageous (e.g. professional-looking photos, information on your extracurricular activities, such as sports or volunteer work), material that portrays you in an unprofessional or controversial light can be detrimental.

Anecdotes, rumours and 'fake news'

- an employer who turned down an applicant after discovering he had used Facebook to criticise previous employers and disclose company information
- a doctor who missed out on a job because the doctor's online activities revealed an interest in witchcraft, and
- a psychiatrist who failed to gain employment after a recruiting agency found explicit pictures of her intoxicated on MySpace
- a nurse working in an older adult care facility posted on her Facebook page that a nurse colleague was about to be fired. The nurse colleague then contacted the nurse manager to find out if this were true. In this case, the nurse manager then had to both discipline the nurse who had made the original posting, and reassure the nurse colleague she was not about to lose her job.

Other issues with employment and study:

Example:

A student took photos of himself in his clinical uniform in the simulation suite depicting inappropriate poses and activities with one of the mannequins. There were also classmates in the background of the photos, which were then posted on the student's Facebook page. The photographed classmates who were also Facebook friends of the student, objected to being associated with his behaviour, both in the simulation suite and online, and complained to the programme leader of the nursing programme in which he was enrolled. The matter was referred to the faculty dean who took disciplinary action against the student.

When using social networking sites, think before making offensive comments or jokes, sharing information about unprofessional activities (e.g. involving alcohol or drugs), or joining or creating groups that might be considered derogatory or prejudiced. Although online groups or web-rings may seem innocuous, other people will not always treat the group with the same humour. Employers, universities, polytechnics and wānanga may access online material and activities about their current nursing staff or students, with potentially career-damaging outcomes.

University/polytechnic/wānanga regulations:

Nursing students are not held to any lesser standards of professionalism than fully qualified nurses – they may face disciplinary action from their universities, polytechnics or wānanga. All nursing students must comply with their university, polytechnic or wānanga regulations and are required to disclose criminal convictions that may prevent their registration with the Nursing Council on completion of their qualification. All candidates for registration as a nurse in must meet the criteria for fitness to practise found in Section 16 of the Health Practitioners Competence Assurance Act (2003). Nursing students consent to the police vetting process again with their application to sit the Nursing Council's state final examination and on employment as a registered or enrolled. The Vulnerable Children Act (2014) requires not only disclosure of convictions but also any other information the police vetting service deems relevant and known by the police.

Booth (2015) collected publicly available tweets of nursing students over a six-day period and analysed them thematically. While these tweets included comments related to the students' education and humour, they also included "vulgar or derogatory comments" and expressions of "anger or stress". Booth outlined the negative impact of tweeting vulgar and derogatory comments that target nursing education programmes and colleagues. The posting of such messages may adversely influence the reputation of an educational institution and have a negative impact on a person's future career (Henning et al, 2017).

In another example, a twitter comment by an Australian medical student, allegedly intended as a joke between friends, resulted in an international media storm for referring to the then United States President Barack Obama as a 'monkey' (Pollard, 2010).

Students are entitled to enjoy an active social life. A study of health professional students, including nurses, found the majority used online media as their primary source of information and over 91 per cent of students aged 18 to 25 used Facebook (Giordano & Giordano, 2011). But remember online behaviour passed off as 'youthful exuberance' at this early stage of a career will still be available later on, and perhaps be seen in a less favourable light. You also need to consider whether your online activities violate university, polytechnic or wānanga regulations and guidelines found in student handbooks (check with your university/polytechnic/wānanga whether it has a policy relating to online behaviour), because this could form the basis of disciplinary action.

Take control of your privacy

Facebook's privacy settings:

The following information regarding Facebook, while specific to that particular site, highlights many of the issues you need to be aware of:

- Facebook changes its privacy settings frequently, so be alert to these sorts of changes in the future.

- You can view and update your privacy controls through settings, which is identified by the grey cog wheel.

- Some features of your profile are considered public information, including your name and profile picture. These features cannot be made private as they are key to having a functional profile. Ways you can be more private online include not having your full name as your profile setting, and having a non-identifying profile picture.

- Other information on your profile can be made private, including your gender, birthday, friends list, photos, geographical location, and pages and networks you associate with.

- The default setting for who can access many types of information on Facebook is 'Public. The 'Public' setting makes information publicly available to any Facebook user and to search engines for indexing purposes.

- You can also control who can see things you post, such as status updates, photos, and other information. This can be done by selecting what privacy level you want the post to be. Privacy levels can be:
    o Public: available to everyone including people who aren't your friends.
    o Friends of friends: your friends list and people who are friends with your friends will be able to view
    o Friends only: Only those you are friends with will be able to view
    o Selected people: You can select specific people on your friend list who will be able to view the post
    o Only me: the post will only be available for you

- Be aware that if you remove content from your profile, copies of that information may remain viewable elsewhere if it has been shared with others. This shared information can still be copied and distributed further.

- Linking third party applications, such as games, photo editors and other apps, you use a Facebook login for, gives the application access to features on your profile. Applications need to gain your permission to gain access. Be wary of applications that ask for full access to your profile, most apps will only ask for specific features, e.g. a photo editing app will ask for access to your camera and photos.

- Your activity on Facebook is monitored under the privacy policy to generate advertisements that target you. Be mindful that friends can also see pages you 'like' and associate with.

- In general, Facebook tries to protect its users from privacy concerns, however this is not guaranteed.

- Further information can be found on Facebook's policies at http://www.facebook.com/terms.php

If you want to know more about how secure your information will be when using online forums, make sure you read their privacy policies. If you still have questions or concerns, you can contact the site operator. Additionally, Aotearoa New Zealand has privacy commissioners with expertise in this area (see www.privacy.org.nz).

Other social media privacy settings:

- Most social media platforms will have changeable privacy settings.
- Be aware that the default privacy setting across many platforms is 'public' meaning that information is accessible to everyone.
- It is recommended you check your privacy settings for each platform you belong to, to ensure your information is kept safe.

Are you maintaining professional standards online?

Online social media challenge: What is 'public' and 'private'?

Even though nursing students and nurses are entitled to a private personal life, online social media have challenged the concepts of 'public' and 'private' and, in turn, changed the way in which online aspects of private lives are accessible to others. Once information is online, it is almost impossible to completely remove and can quickly spread beyond a person's control. A moment of rashness now could have unintended and irreversible consequences in the future – inappropriate online activities can be detrimental to relationships with patient/client and colleagues, training and employment prospects, and personal integrity. This is not to say nurses should avoid using social media, because their use can be personally and professionally beneficial. Traditional expectations regarding the conduct of the nursing profession still apply in this non-traditional context; nursing students and nurses always have a duty to patient/client and the community to maintain professional standards, including when using online social media.

Example:

A Canadian nurse Carolyn Strom was disciplined and fined by the Saskatchewan Registered Nurses Association (SRNA) after a 2015 Facebook post that criticised the end-of-life care her grandfather received. She was on parental leave at the time and the post was on her personal Facebook page.
Staff at the facility in which her grandfather had been cared for complained to the SRNA which found Strom guilty of professional misconduct and fined Strom $1000 for violating the organisation's code of ethics and ordered her to pay $25,000 to cover some of the costs of the investigation and hearing.
An appeal in 2018 to the provincial court upheld the SRNA's decision.
http://thestarphoenix.com/news/local-news/sask-facebook-nurse-carolyn-strom-loses-appeal-of-26000-fine-by-srna

---

Since the Christchurch earthquakes, some DHBs have established organisational Facebook pages but have not established policies for use by staff. The linking features of Facebook pages mean personal information becomes visible on an organisational Facebook page without an individual realising it.
Be vigilant regarding photos. A simple photo taken by a smartphone can be downloaded and shared on social media in a matter of moments. Never post a photo online without the express permission of the person/people who are the subject of the photo and also the people who may be in the background and identifiable from the photo.

Troubleshooting: Have you ever…?

- Googled yourself?
  - Search for your full name in Google, particularly 'New Zealand Sites Only'. Do you feel comfortable with the results that are shown?

- Googled a patient/client, perhaps in an emergency situation?
  - How have you used this information?
  - Were you able to establish with the patient/client concerned that the information found was current/accurate?

- Posted information about a patient/client or person from your workplace on Facebook?
  - Had a look through your old online posts and blogs.

- Added patient/client/client as friends on Facebook or any other social media platform
e.g. Twitter or Instagram?

- Added people from your workplace as friends?

- Made a public comment online that could be considered offensive?

- Become a member or fan of any group that might be considered racist, sexist or otherwise derogatory?
  - Browse through all the groups you have joined and consider whether these are an accurate reflection of the person you are, and the values you hold.

- Put up photos or videos of yourself online that you would not want your patient/client, employers or people from your workplace to see?

- Checked your privacy settings on Facebook or any other social media platform?

- Felt that a friend has posted information or images online that may result in negative consequences for them?
  - Did you let them know?

References

Adhesion Online. (2018) Social Media Usage in New Zealand 2017 to 2018. Retrieved from https://www.adhesion.co.nz/blog/social-media-usage-in-new-zealand

Booth, R.G. (2015). Happiness, stress, a bit of vulgarity, and lots of discursive conversation: A pilot study examining nursing students' tweets about nursing education posted to Twitter. *Nurse Education Today*, *35*(2), 322–327.https://doi.org/10.1016/j.nedt.2014.10.012

Brown, V. R., & Vaughn, E. D. (2011). The writing on the (Facebook) wall: The use of social networking sites in hiring decisions. *Journal of Business and Psychology*, *26*(2), 219.
Retrieved from https://link.springer.com/article/10.1007/s10869-011-9221-x

Chester, A.N., Walthert, S.E., Gallagher, S.J., Anderson, L.C & Stitely, M.L. (2017) Patient/client-targeted Googling and social media: a cross-sectional study of senior medical students. *BMC Medical Ethics* 18:70 DOI 10.1186/s12910-017-0230-9. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5715642/

Gilpin, C. (2017). Will Social Media Help or Hurt Your College and Career Goals? Retrieved from https://www.nytimes.com/2017/02/24/learning/will-social-media-help-or-hurt-your-college-and-career-goals.html

Giordano, C., & Giordano, C. (2011). Health professions students' use of social media. *Journal of allied health*, *40*(2), 78-81. Retrieved from http://www.ingentaconnect.com/

Graham, N. & Moore, P. (2008).The Dangers of Facebook. *Student BMJ;* 8:10, 354-355. Retrieved from http://student.bmj.com/student/view-article.html?id=sbmj.a1658

Henning, M., Hawken, S, .MacDonald, J., McKimm, J., Brown, M., Moriarty, H., Gasquoine, S., Chan, K., Hilder, J., & Wilkinson, T. (2017) Exploring educational interventions to facilitate health professional students' professionally safe online presence. *Medical Teacher 39*(9), 959-966.

Medical Council of New Zealand (2016) *Statement on the use of the internet and electronic communication.*
Retrieved from https://www.mcnz.org.nz/assets/News-and-Publications/Statement-on-use-of-the-internet-and-electronic-communication-v2.pdf

Ministry of Justice. (2015). *Harmful Digital Communications Act.* Retrieved from http://www.legislation.govt.nz/act/public/2015/0063/latest/DLM5711810.html

Ministry of Justice (2000). *Employment Relations Act.* Retrieved from
http://www.legislation.govt.nz/act/public/2000/0024/latest/versions.aspx

National Council of State Boards of Nursing (2018) *A nurse's guide to the use of social media.* Chicago Retrieved from
https://www.ncsbn.org/NCSBN_SocialMedia.pdf

New Zealand Nurses Organisation. (2010). *Code of ethics.* Wellington: New Zealand Nurses Organisation.

New Zealand Nurses Organisation. (2012) *Standards for professional nursing practice*. Wellington: New Zealand Nurses Organisation.

Nursing Council of New Zealand. (2009) *Code of Conduct.* Wellington: Nursing Council of New Zealand.

Nursing Council of New Zealand. (2010). *Education programme standards for the registered nurse scope of practice.* Wellington: Nursing Council of New Zealand.

Nursing Council of New Zealand. (2012a) *Guidelines on professional boundaries.* Wellington: Nursing Council of New Zealand.

Nursing Council of New Zealand. (2012b) *Guidelines: Social media and electronic communication.* Wellington: Nursing Council of New Zealand

Nursing Standard. (2010) Nurse struck off after Facebook link with patient/client. *Nursing Standard, 25*(2) p.11. Retrieved from https://rcni.com/nursing-standard

Pollard, E. (2010). Young Lib expelled over Obama monkey slur.

Retrieved from http://www.abc.net.au/news/2010-04-16/young-lib-expelled-over-obama-monkey-slur/399176

Other Resources

ICN Nurses and social media (2015)

RCN - Getting started on Twitter
Guide for those who are new to Twitter on how to use this social media site effectively, with information on registering for an account, using hashtags, mentions and direct messages as well as top tips for getting noticed.

https://www.rcn.org.uk/professional-development/publications/pub-005031

RCN Guide to blogging

This guide is for RCN members who would like to write an informal piece about something affecting nursing or their specialty through the RCN's blog pages. It gives clear instruction on how to start a blog, what to include and how to get it published online.