Engineering UTC Northern Lincolnshire

Social Networking Guidance

Document control table

Document title:	Social Networking Guidance
Author (name & job title):	Anesta McCullagh, Principal
Acknowledgement	
Version number:	V4
Date approved:	Approved March 2025
Approved by:	Approved by UTC Board
Date of review:	March 2026

Document History

Version	Date	Author	Note of revisions
V4	March 2025	NBD	Updated links

1. Social Media

1.1 The open nature of the internet means that social networking sites can leave professionals, such as teachers vulnerable if they fail to observe a few simple precautions.

1.2 We use the term 'social media' to describe any kind of web-based tool that you can use for sharing what you know, including but not limited to: blogs, photos, videos, social networks, mobile phone applications, text, email, digital TV services, wikis, gaming and collaboration tools.

1.3 More and more people are registering with and using social networking sites like Facebook to stay in touch with friends & families. Online social networking sites are growing at a great speed and being more accessible as a means of communication.

When used appropriately, online social networking sites can be a great way of finding old friends, sharing information, staying in touch with friends & families and joining interest groups.

1.4 In today's world, work is a very big part of our lives, so it is only natural that people discuss to some degree their public life in private in online conversations. However, employees should be careful as these online conversations are stored permanently and searchable by the public. In other words, it is in the public domain, and can be used by employers against staff if they feel that you have acted inappropriately or breached confidentiality.

1.5 Like in any other profession, you have a right to a personal life. Using online social networking sites whilst fun can be hazardous, and confidentiality can potentially be inadvertently breached if employees discuss personal and sensitive things relating to work in online conversations. Some employers are concerned about this and if confidentiality is breached this could be seen as bringing the employer into disrepute.

1.6 Most sites allow you to create a profile yourself. This can be as simple as a username and contact email address, or it may include a photo, a description of you, likes and dislikes, music and videos. It may also link it your online friends' profiles. It could be seen by thousands of people and not everyone will agree with what you write.

1.7 When posting on websites, it is also worth thinking about the impression you're creating – would the things you write or the pictures you post cause embarrassment in real life? How would you feel if a potential employer or students and their parents saw things you had posted? Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.

1.8 Be careful about the personal details you post online. Little bits of information can be used by others to build up a picture of you that could be misused. Don't reveal your home address, telephone number, date of birth or where you work, use a generic term such as education, or leave the options blank where possible. Identity theft is a crime on the rise with criminals using such information to access bank details.

1.9 Keep your password safe and avoid obvious ones that others may guess, particularly if you also use it for other things. It's worth having a separate email address just for social networking so you don't have to giveaway any other contact details.

1.10 Do not make disparaging remarks about your employer/colleagues. Doing this in the presence of others may be deemed as bullying or harassment and there are examples of when it has led to dismissal.

1.11 Act in accordance with your employer's information technology (IT) policy and any specific guidance on the use of social networking sites. If your college provides guidance on what is considered to be appropriate contact with students, follow it. Having a thorough policy in place helps staff and students keep within reasonable boundaries.

1.12 Other users could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed. You could face disciplinary action as a result of being 'tagged'. Photos and text from your profile can be copied and edited by others, like anything else on the internet.

1.13 Parents and students may access your profile and could, if they find the information and/or images it contains offensive, complain to your employer.

1.14 If you have any concerns about information on your social networking site or if you are the victim of cyber bullying, you should report it immediately.

1.15 Be aware of what monitoring, if any, may be carried out by your college. Full details should be outlined in the IT Policy.

2. Policy for Staff

If you are using Social Networking or Instant Messaging sites:

2.1 Do not correspond with students or parents/carers or have them as your 'friends/contacts'. It is essential that you maintain a professional distance between yourself and your students and their families.

2.2 Do not request, or respond to any personal information from a child, ensuring that communication only takes place within clear and explicit professional boundaries through the college's own communication channels.

2.3 If a 'friend/contact' makes a comment that you find offensive – delete them. Otherwise it could be considered you agree with them.

2.4 Do not include personal details such as email address, telephone number, date of birth – possibly use a different name.

2.5 Never give students your personal email address, telephone or other contact details, always use approved college communication routes.

2.6 Ensure your privacy settings have been configured as securely as possible.

2.7 Always consider what you post on your site and whether you would be happy for this to be seen by your students, the community or your employer.

2.8 Stay within the legal framework and be aware that defamation, copyright and privacy laws, amongst others, apply.

2.9 Do not correspond with former students unless they have been beyond college age for more than 2 years. Remember that children up to the age of 18 are covered by safeguarding regulations and therefore contact with former students could still be seen as inappropriate.

2.10 Be aware that any photographs which have been posted can be copied and amended, as can any text you have written.

2.11 Be aware that your friends may upload photographs of you and tag them with your name – suggest you edit them first.

2.12 Remember that if you make a comment on one of your friends/contacts' site then they may not have the same level of privacy settings as you and that this comment may be publicly accessible.

REMEMBER

What you say online is there forever even if you subsequently delete it. Therefore, what you may believe is said privately on a social networking site may, at some point, become public.

3. Privacy Settings

3.1 Any decent social networking website should have clear and visible privacy settings. They can usually be accessed from the homepage of your account, along with other general options. You can adjust your privacy settings to control who can see your information, and how much they can see. The below guidelines are not intended as a set of instructions, but general advice on how to avoid compromising your professional position.

3.2 Consider using the highest privacy settings when you first create your profile, then gradually adjust them and allow networking features only when you feel comfortable. This way, you won't be making information available unless you really want to.

3.3 Think about what you want to use your profile for. If you only want to keep in touch with family and close friends, set your profile up so that it can only be accessed by those people.

3.4 You can set up your profile so that people can only access it if you have approved them. Once you accept someone as your friend, they'll be able to access all the information and photos you have on your profile. You can always remove friends or followers if you change your mind but by then they may have already seen your details.

3.5 On some social networking sites, people that aren't your approved friends will still be able to see some details on your profile. It's worth checking what they will be able to see. On Facebook, you can choose to make people 'limited friends', so they will only have access to a cut-down version of your profile.

3.6 If you don't understand how to adjust your settings or you feel that you aren't being given enough options, get in touch with the site administrator or customer service team. If you still aren't happy, consider not using the website.

3.7 To ensure that your Facebook account doesn't compromise your professional position, ensure that your privacy settings are set correctly.

3.8 Do not under any circumstances accept friend requests from a person you believe to be either a parent or student at your college.

3.9 Always make sure you log out of Facebook after using it, particularly when using a machine that is shared by other colleagues/students. Your account can be hijacked by others if you remain logged in – even if you quit your browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Make sure you clear your chat history on Facebook (click "clear chat history" in the chat window).

3.10 Employers may scour websites looking for information before a job interview. Take care to remove any content you would not want them to see.

A

Setting	Recommended Security Level
Send you messages	Friends Only
See your friends list	Friends Only
See your education and work	Friends Only
See your current city and hometown	Friends Only
See your likes, activities, and other connections	Friends Only
Your status, photos, and posts	Friends Only
Bio and favourite quotations	Friends Only
Family and relationships	Friends Only
Photos and videos you're tagged in	Friends Only
Religious and political views	Friends Only
Birthday	Friends Only
Permission to comment on your	Friends Only posts
Places you check in to	Friends Only
Contact information	Friends Only

minimum

Recommendation for Facebook privacy settings:

- Stop the network provider from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding you details, click "Privacy Settings". Under "Applications and Websites" click "edit your settings". Scroll down to "Instant Personalisation" and make sure the checkbox for "enable instant personalisation on partner websites" is unchecked.

4. Cyber Bullying and Harassment

4.1 If you are the victim of the above by students, parents/carers, colleagues or other individuals with whom you have a professional relationship follow the steps outlined below:

- Where possible, save the evidence for future reference using screen shots etc. Keep a record of what and when.
- Report the problem to the service provider.
- Contact you line manager, SLT and/or the Principal to inform them of the situation.
- You may also wish to involve the Police.

4.2 These guidelines also apply if students report bullying or harassment, it is vital that Parents are informed and the Police in cases of suspected inappropriate conduct by an adult.

5. USING SOCIAL MEDIA IN YOUR WORK

5.1 The college would like its employees to feel confident when using social media and to achieve meaningful results through these activities. This policy has been developed to help employees understand good practice for online participation and to make clear the standards expected of anyone using social media.

5.2 This policy is in addition to any professional standards that govern specific areas of work for employees and in addition to all other college policies.

5.3 This policy should be followed in conjunction with any code of conduct, which describes the standards of conduct and practice that the college's employees should follow. The code is a key element in the employment relationship and therefore an integral part of the contract of employment.

5.4 Social media should be seen as another communication channel in the same way as telephone and e-mail and therefore the same behaviour and activities should be observed. However it is important to note that unlike telephone and e-mail exchange information posted on a social media site is publicly available.

5.5 Furthermore each employee using social media for work purposes must receive sufficient training and support.

5.6 Before using social media you must have received the necessary permission or appropriate delegation, in writing, from your head teacher. This will detail which social media you can access during work time. You should then follow these guiding principles for any social media activities that are part of your work:

5.7 **Be responsible for your actions**

Remember that you are a representative of the college. Where possible you should disclose your position as a representative of the college but consideration should be given to personal safety when doing so. Using social media on behalf of the college means that you are responsible for your own actions and may be held accountable for these. Conduct that

is likely to bring discredit to the college will be dealt with in accordance with the college's disciplinary procedure.

5.8 **Be respectful**

Set the tone for online messages and conversation by being polite, open and respectful. Use familiar language and be cordial and professional at all times. You must ensure that you respect people's confidentiality and do not disclose non-public information or the personal information of others. If you are unsure what information is in the public domain then always seek clarification before divulging anything. Respond to questions and comments in a timely manner, ensuring you meet the users expectations for the type of social media you are using.

5.9 **Be credible and consistent**

Ensure accuracy of information; be fair, thorough and transparent. Encourage constructive criticism and feedback.

5.10 **Be confident**

Don't be scared of participating but if in doubt always seek further guidance before doing so. Never publish anything you are unsure about and be confident and clear in what you say.

5.11 **Be integrated**

Wherever possible, align online participation with the college's website and other offline communications e.g. college magazine/newsletter.

5.12 **Be legal**

Remember that laws relating to defamation, copyright and data protection apply when using social media (other laws may also apply). You should not make statements about other people or companies that could harm their reputation, and you should be careful not to copy the work of another person or company as this could be a breach of copyright laws. Personal information about other people should not be placed on social media as this is their information and any such disclosure of personal information could be a breach of the Data Protection Act/General Data Protection Regulations 2018. The college can be held liable for your actions so if you are unsure about whether you are acting within the law you should seek further legal clarification.

5.13 If you need advice about using social media in your work, then get in touch with others who can help you – the sooner the better. You can make good use of the expertise within the college and learn from other people's experiences.

5.14 The college's social media business accounts are not to be used for personal reasons. Unauthorised entry into the college's computer systems, unauthorised use of software or breach of the data protection requirements is a breach of the college's disciplinary rules.

References

Social Networking Advice – ICO Youth Information Commissioner's Office, Online safety | ICO

Social Networking – Guidelines for Members National Association of Schoolmasters and Union of Women Teachers (NASUWT) NASUWT | Protecting Your Privacy Online