Can I be friends with my pupils on social networking services?

A recent TES survey found that a small percentage (9%) of teachers were friends with their pupils on SNS. It is not a good idea to accept friend requests on your personal accounts or to accept requests to follow you from pupils, recent pupils or even parents at your school. On most services, the sender won’t be notified if you select ignore/not now or delete for such requests, nor, if you had already accepted such a request, will they be notified if you remove them from your friends list or followers. By accepting such requests you could be making yourself vulnerable by sharing personal information or by having access to personal information about your pupils. You may be potentially leaving yourself open to allegations of inappropriate contact or conduct or even finding yourself exposed to unwanted contact. Your school may provide guidance regarding this in their E-safety or Acceptable Use Policy (AUP) and there is clear guidance supported by the Teaching Unions to say that friending pupils is not appropriate.

Some educators and schools do use Facebook or other SNS to connect and communicate with pupils, parents, and governors, but they do so using professional or organisational accounts or pages, with prior approval from their Senior Leadership Team (SLT) and recognising that Facebook and many SNS do have a minimum age-requirement of 13.

Which privacy settings do I need as a teacher if I am using social networking services?

The answer will depend on what you have on your profile, and what you tweet or post. It is important that when using SNS you are in control of who can see your account details and content including photos and albums, posts, status updates and any personal information. On Twitter, you can set your account to private by selecting ‘Protect my tweets’ so you can then accept (or decline) requests to follow you. In the case of Facebook, choosing a basic ‘friends’ setting for every option would initially achieve this. However, you are able to customise each option further, and can limit the information that certain individuals see. It is a good idea to use the “view as” option, to check and see how your profile appears to strangers, and that the information you want to remain private or ‘friends only’ is not visible. If you are unsure about how to use the settings available, treat all information that you post as being public and act accordingly.

Think carefully about whom you are friends with, and which friends can access what information. It is a good idea to remove any “friends” or customize the privacy settings for current friends, if access to your personal activity could compromise your position, for example parents with children at your school. However, whatever setting you use, it’s important always to think before you post because ‘friends’ settings do not guarantee privacy. Sharing content with others could mean that you lose control of it, if friends pass on your information, for example.

Think carefully about comments you post on friends’ walls – if their profile is not set to private your posts will be visible to anyone.

What about the use of geo-location services?

Geo-location services are beginning to be used by educators to support teaching and learning. However, there are obvious issues in making sensitive information – where you are at a given time or the places you regularly visit – public. When using location services on SNS, think about making your location visible to only your friends and ensure that you are happy with the friends in your list. The option for being ‘checked into’ a place by someone else can be disabled in your privacy settings, so you can keep control of your location information.
4. How can I continue to protect my professional reputation?

» Your professional reputation is clearly valuable to your current and future career and consequently managing your online reputation is an essential part of being a teacher. Always think carefully before making any posts, status updates or having discussions regarding the school, its staff, pupils or parents in an online environment – even if your account is private. Comments made public could be taken out of context and could be very damaging. Think about the language you use – abrupt or inappropriate comments, even if they were made in jest, may lead to complaints. Anything that is put online is potentially public and permanent.

Posting derogatory comments about pupils, parents or colleagues is never acceptable. Teachers are required to uphold the reputation of the school, to maintain reasonable standards in their own behaviour, and to uphold public trust in their profession. Bringing your school or your profession into disrepute may cost you your job.

» Use a strong password, and log out of the SNS after using it. Not logging out means the next user of the computer or other access point can access your SNS account. (Deleting cookies may be necessary if you had selected the ‘remember this password’ option when you were logging in). If you access social networking via an application on your mobile phone, it is a good idea to set a PIN or passcode for the phone, and to remember to log out of the SNS app after each session, so if you mislay your phone, access to your SNS account is still protected.

» Be mindful of how you present yourself when you are choosing a profile image, for example, or even when joining a Group or ‘liking’ pages – think about what these choices say about you.

» Consider making private, or removing, previous online content that might compromise your current position. It is possible to deactivate existing SNS accounts and to permanently delete profiles. It is important to be aware, however, that though such changes will be immediate on the service itself, content which was visible on public search may still be visible on public search results for a week or two (or even longer!) until these changes have been recognised by the search engine.

» Searching your name regularly on public search engines can be a useful way to monitor your online content or ‘digital identity’. Other tools are also available, for example, utilising privacy settings and removing your profile page from a search engine result. Your online reputation is important for your current and future employment – it is common for employers to search prospective employees online. One recent survey found that 41% of employers in the UK rejected candidates due to data found online.

5. What should I do if other people post inappropriate images of me online? How about if I am the victim of cyberbullying?

If you are unhappy with photos in which you are tagged, untag yourself or alternatively contact the friend and ask them to remove this content. Never be shy about asking others to take down or make private content that identifies you that you are not comfortable with. Be thoughtful about content you post that relates to others, and respond positively to requests to take down or make content private. If you think that the image or video breaks the SNS’s terms of use, report it to the SNS who can take content down (look for the Report Abuse options in the service).

If you are the victim of cyberbullying, for example, a pupil makes inappropriate comments or posts images of you or another member of staff, don’t retaliate and save/print all available evidence (wall posts, URLs, messages, comments etc). Schools have a statutory duty of care for the health, safety and welfare of school staff and should therefore take reasonable steps to support staff experiencing cyberbullying. Your school should have a reporting line or procedure in place, and this process should take into account cyberbullying incidents. Appropriate points of contact within your school may include your mentor, line manager or the SLT lead in this area. Staff can seek additional support and advice outside of the school; contact your Union or professional association, the Teacher Support Network or the Professionals Online Safety Helpline.

6. What should I do if I see inappropriate content on social networking sites about my pupils?

If you come across, or are made aware of, inappropriate use of social networking sites by your pupils (including under age use of these services), you should report these to the appropriate person within your school – the school point of contact for safeguarding and/or the Head of Year/ member of SLT with responsibility for behaviour. The school should have a range of policies and procedures, including its Behaviour Agreement and AUP, which relate to the inappropriate use of SNS by pupils.

7. Can I use sites like Facebook or Twitter in school for educational purposes with my pupils?

Most SNS have an age requirement of thirteen. Social networking services are blocked in many schools. However with careful planning and management, they can be used responsibly by educators to provide valuable opportunities for collaborative learning. There has been work reviewing the potential benefits of using SNS with learners, and SNS use in education alongside other technologies. For example see the Cloudlearn.net project, and ‘Using Facebook in the Classroom’. If your school supports the positive use of SNS, always seek clear guidance from a senior member of staff if you wish to use these with your pupils. Always act in accordance with school policy.

Further information

Cyberbullying Guidance – supporting school staff
www.digizen.org/resources/school-staff.aspx
Facebook Safety advice for Educators
www.facebook.com/help/?safety=educators
Young people and social networking sites – a guide for parents, carers and teachers:
Using Facebook safely: A guide for professionals working with young people published by the Yorkshire and Humber grid for learning:
http://tinyurl.com/4yumwv

4 See www.microsoft.com/presspass/features/2010/jan10/01-26dataprivacyday.mspx
5 See for example, http://www.digizen.org/socialnetworking/benefits.aspx, and see for example, ‘33 Interesting Ways to Use Twitter in the Classroom’ https://docs.google.com/present/view?id=dlhav2cv5_1t8cb8mf8
6 See www.heppell.net/facebook_in_school