Social media guide for staff

There are so many positives to social media; it's an effective medium for communication, a source of information, a platform on which you can have your say. However, when not used correctly, there can be negatives. Alan Mackenzie, of e-Safety adviser, explores the rise of social media and offers some sage advice on how best to manage it in and out of school

Social media taps into one of the fundamental aspects of being human; our appetite for social interaction. The very nature of these interactions means that we have access to an incredibly diverse array of content, thoughts and opinions – the very best of humanity and, unfortunately, the very worst too.

Whether you like it or loathe it, it's here to stay, and it's immensely popular from both a personal and professional perspective – and schools are no exception. Increasingly, professionals are using social media in a pseudo-professional capacity – using a personal account but also engaging and collaborating with others about professional matters; there's nothing wrong with that as long as simple boundaries are adhered to.

FILTERING THROUGH TO MAINSTREAM ACCEPTANCE

For many years I have been a huge supporter of the use of social media for parental and community engagement and, over that time, it has been interesting to see how attitudes have changed. In the early days, I was told anything from 'You should know better!' to 'Why are you promoting paedophiles?' These statements and others were from educational professionals – largely from people who had never used any social network and had only ever heard bad things about them.

But time has moved on, attitudes are changing, and more and more schools are using social media very effectively. Equally, more members of staff are using social media in a personal capacity and so it's important to reiterate to staff your professional expectations. Whilst all members of staff have a right to use these platforms, September is a timely period to remind everybody that, as professionals working with children, the behavioural expectations are higher than in many other professions and this comes down to your school's code of conduct. You should also consider briefing new members of staff as part of their induction.

DEFINING BOUNDARIES AND EXPECTATIONS

In the context of this article I'm not a great fan of black and white rules – I think boundaries and expectations with a degree of flexibility and good old fashioned common sense should play a significant part. For example, 'Staff should not be friends with, or interact with, children or parents of children.' In theory that might sound perfectly acceptable but what if you are a small community school where some of the staff are also 'real' friends with other parents? Such a rule simply wouldn't work; flexibility is needed.

So I would like to share some very simple but important points that you can raise with staff. These points can also serve as a checklist to ensure your code of conduct meets your needs or as part of a staff training discussion. ▶

Social media code of conduct

1. Think before you post

1. Think before you post

Isn’t that something we teach children? Yes, but for something that sounds so simple it is one of the most important points for adults too. For children the message is predominantly about safeguarding (depending on age) but for adults it impacts on other areas as well, such as:

- conduct
- reputation (personal as well as school reputation)
- data protection.

To simplify:

- Be critical about the content you are posting. That joke, video, opinion, meme, can easily be taken out of context by others; what you say is not necessarily what others read. Equally, be mindful of discussing school business or even mentioning the school by name.
- Consider who you have contact with. Students are a definite no (in a personal capacity) but the school should make its expectations clear about boundaries and any flexibility within these.

A cyber-psychology theory called ‘online disinhibition’ plays a big part here. If you’re interested (safeguarding lead, pastoral care, online safety lead, etc.,) have a look online at this paper by Professor John Suler called *The Online Disinhibition Effect*.

2. Privacy settings

2 Privacy settings

Check privacy settings and use them wisely. Privacy settings are not a total solution; there is no such thing as absolute privacy online – for example, screenshots can be taken and shared. I have seen more than one report in the past where someone (invariably a student) has created a false profile pretending to be a member of staff, managed to get into a private group chat and taken part in discussions about other students, members of staff etc.

Most privacy settings are very easy to use (on or off), but some are not so easy, the perfect example being Facebook which has many different settings. Learn how to use them properly. Remember that just because your account is set to private doesn’t mean that everything is private. Profile information such as profile picture and other information can still be seen regardless of the privacy setting.

Occasionally check those privacy settings. It’s a myth that privacy settings are disabled whenever new features or changes are made to certain social networks such as Facebook.; years ago this used to happen on occasion but that’s very rarely the case anymore. More likely a new feature is added and the privacy of that feature defaults to off (or open); occasional checking allows for a level of reassurance.

3. Know where to go for help

3. Know where to go for help
Unfortunately, incidents or breaches do happen. There are some people who think they have a right to freedom of expression which, to them, means they can say anything they want. On occasion, this can overstep the boundaries of legality into harassment, intimidation, defamation, etc. As a school you need a means to support your staff.

Reporting such incidents to the social network and blocking is the most appropriate course of action. However, unless it breaches their regulations, the reality of that social network doing anything about it (unless you're famous) is unlikely. There are times when you will need to seek advice from the police and/or the local authority or trust legal team.

4. Regularly search yourself

4. Regularly carry out a search on yourself on the more popular search engines such as Google (e.g. your name, any profile/pseudo names you use)
This is an incredibly useful thing to do and, what's more, it's easy and you can arrange to receive automated email alerts – Google Alerts – once a day, once a week or another time period that suits you best. Many schools are taking advantage of Google Alerts in order to be made aware of any issues that may affect the school reputation.

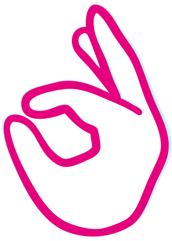
Similarly, individual staff members can have alerts set up in order to keep a watchful eye on any mentions of them on the internet. Google searches are not a complete solution, they certainly won't find everything, but for something that is free, and so simple to use, it's a very effective tool in the toolbox.

5. Don't forget your digital housekeeping

5. Every now and again carry out some digital housekeeping; I do it annually
Over the course of a year – depending on your usage – you can accumulate a huge amount of digital junk. This includes new social media services you've been testing, old pictures and videos you may have posted, etc. Have a look through and take a little time to reflect. Do you still want that information up there? Do you still need those old accounts?

Something that many overlook is how many online services they sign-in to using their social media login details (e.g. Facebook, LinkedIn). Go through the 'allowed apps' within that social network and make sure you know which services you are allowing to access your data. Delete any you don't know or don't need anymore.

Hacking is big business. It isn't uncommon to see third-party services being hacked in order to find personal information. These third-party services may be services that you have used with your social media login details (which is why you need to check the 'allowed apps'). When you initially set up this social media account you may have used a personal email address to do so. Check your email address on the Have I Been Pwned website (the spelling is correct).



**I've kept these points purposefully simple – there's no need to overly complicate things.
These will cover you personally and professionally in the vast majority of circumstances but, if something happens and you're not sure what to do you, can always ask for help there's plenty of advice online.**