



INTRODUCTION

Social media services like Twitter, Facebook and WhatsApp have very quickly become a part of our lives; changing the way we keep in touch with friends and family as well as the way we share ideas and get information. This guide is designed to support your personal and professional use of these services in order to keep pupils, yourself and your job safe.

NOTE: For guidance on setting up an account for your department or school and managing your schools online read LGfL's Online Reputation Management for Schools -

onlinerep.lgfl.net



Managing your school's online reputation - If you don't, someone else will



PRIVACY SETTINGS

Whilst it is important to remember to think carefully about the things you share online - because they may be shared by others - social media sites have privacy settings and safety features to help you manage who can contact you and see the things you share online.

Should I make all my social media accounts private?

The key is to determine what you want to use that particular social media account for and then decide:

PERSONAL USE

If you are using social media in your personal life you should make the account private. In most cases, if an account is private all someone will be able to see is the account name and profile picture.

- ☐ Make account private
- ☐ Use a different name or variation of your name
- ☐ Use an appropriate headshot or picture

PROFESSIONAL USE

If you are using social media to network, share your ideas, showcase achievements and discuss issues you can make your account public. If you are public, remember that anyone can see what you post.

- ☐ Account could be public or private
- ☐ Use your name and/or subject eg MsSmithICT
- ☐ Use an appropriate headshot or picture

What should I use privacy settings for?

Securing my personal information

Social media sites are all about sharing and this could include some of your personal information. Use the settings to control how much appears on your profile and who can see it. For advice on security for your accounts and devices please see our [Using Technology Safely Checklist](#).

Customising who I share posts with

Some sites allow you to create groups or you can even select specific friends to share that particular post with.

Controlling who can contact me and make friend requests

If your account is public this usually also means that any user can add you or even just view the posts you are sharing. Locking your account down to private will mean that you will be sent a request when someone wishes to follow you which you can accept, decline or ignore.

Keeping your location private

Social networks allow you to tag your location to your posts (ex. on holiday or at a restaurant) but it is important to remember that your location is key personal information. You do not have to add your location to posts and you can also prevent social media from accessing your location at all through the privacy, location or app settings.

Tagging

Your name could be tagged in a photo or on a post you would be interested in. This is great for finding things quickly but ultimately this can lead to these posts being seen by a far wider audience. You can use the settings to make sure you have to approve tags or are notified whenever somebody tags you.

For more detailed information on **privacy settings** and how to set them up for the main social media sites visit:

www.saferinternet.org.uk/safety-tools

Be aware that if you are on a **school trip** with pupils you should not share location information to ensure their safety.



Scenario

A pupil has found holiday photos of you on a social media account and shared them with their friends. Here is our advice...

Evidence	Note down what happened and who is involved. Screenshot or take a photo of anything relevant.
Tell your school	It is best to let your school know as soon as possible so that they can talk to the pupils involved and to prepare them if there are any complaints.
Find the source(s)	Find the photos and make them private or remove them if you wish. If hosted on a friend's account ask them to take them down. Consider making all your accounts private and removing any photos that could impact your professional reputation
Seek further help	Call the Professionals Online Safety Helpline (POSH) for any further help and advice on 0844 381 4772 or email: helpline@saferinternet.org.uk



MANAGING YOUR PROFESSIONAL REPUTATION

Search and search again

The best way to find out your online reputation and **test your privacy settings** is to search for yourself regularly on a search engine.

If you do find any negative or upsetting posts that will impact your professional reputation then save the evidence by taking a photo or screenshot and tell your school. Do not reply or comment on the post.

Instead use the reporting procedures of the site(s) involved and contact the **Professionals Online Safety Helpline** for advice. If you find an account that has been set up in your name then you should also tell your school and report to the social media site it is on. When reporting make sure you add as much information as possible.

For more help and guidance on reporting please visit:
www.childnet.com/resources/how-to-make-a-report

TOP TIP

When searching, use your name and location first then check variations of your name and even try nicknames.

IMPORTANT

Social media sites often update their privacy settings and may add new features. Revisit your settings on a regular basis to check.

Unsure about how to use the settings available? Treat all information that you post as being public and then act accordingly.

Think before you post

Is that photo appropriate? Could that joke be seen as offensive? Should you respond to that comment you did not agree with? Be mindful when sharing pictures or posts or liking content online which could bring your reputation or that of your school into disrepute. Hashtags can link your content to other content with the same hashtag. **#BeAware**

What about the things my friends and family share? How do I talk to them?

With social media you are only as private as your most public friend. You may have a friend who loves to share all aspects of their life online and that affects you. It is worth talking to them about privacy settings and being mindful of your professional reputation.



INAPPROPRIATE CONTENT ON SOCIAL MEDIA INVOLVING YOUNG PEOPLE FROM MY SCHOOL

The key message here is to tell your school. Certain issues like cyberbullying and self-harming would be a matter for your school's Designated Safeguarding Lead. If you were to see this or inappropriate comments about the school or staff you should take screenshots or photos as evidence and inform those responsible for behaviour in your school. If you see a young child on social media that are putting themselves at risk you should also report this to your school.

If the content which you see online may be an example of sexting then we recommend you refer this immediately to your Designated Safeguarding Lead. For more information on handling incidents of sexting please refer to the [UKCCIS Sexting Guidance for Schools and Colleges](#).



RESPONDING TO FRIEND OR FOLLOWER REQUESTS FROM PUPILS

Current pupils

We recommend declining the request and most school policies will state that you should not accept friend requests from current pupils. If you are receiving frequent requests from the same pupils then speak with your Senior Leadership Team or consider blocking the pupils to prevent further requests.

If pupils are under the age of 13 (the age that most of the popular social media companies have to legally comply with) it is worth asking the young person if their parents or carers know they are using social media and checking they know how to keep themselves safe.

What about former pupils?

Pupils from a previous school, those who have moved schools or who are now adults may not be covered by your school's policy. Whilst you are not their teacher or support worker any more you should think very carefully before accepting their request. Young people may have younger siblings or friends still in the school too so we would recommend that you do not accept the request.



Scenario

You receive a friend request from a colleague who is also the parent of one of the pupils you teach.

What is the school policy? Always be clear on your school's policy and follow it.

What could go wrong? Pupils and other parents may be able to see your content through this colleague.

How to decline This is a socially awkward situation but your colleague should understand this. Reply online and explain your concerns or talk to them. If your school has a clear policy on this then you could make your colleague aware of this.



Further information

Childnet - Teachers and Professionals section www.childnet.com/teachers-and-professionals

UK Safer Internet Centre- Teachers and school staff section www.saferinternet.org.uk/advice-centre/teachers-and-school-staff

Social media guides www.saferinternet.org.uk/safety-tools

Childnet – Using Technology Safely Checklist www.childnet.com/resources/educators-pack-for-online-safety-awareness

Professionals Online Safety Helpline (POSH) 0844 381 4772 or email: helpline@saferinternet.org.uk

Childnet - How to make a report www.childnet.com/resources/how-to-make-a-report

UKCCIS Sexting Guidance for Schools and Colleges www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis



Childnet
International



UK Safer
Internet
Centre



Co-financed by the Connecting Europe
Facility of the European Union