Sidney Stringer
Multi Academy Trust

Social Media Advice to Staff

September 2016 – September 2018

Social media sites such as Facebook, Instagram and Twitter are continuing to gain in popularity, but as a public site pose risks to staff. There have been a number of cases in the news where members of staff have ended up facing disciplinary action because of posts or activity on social media. These have included:

- A teacher who posted comments about weekend drinking parties. Even though this was nothing to do with school, pupils found it and read it. The school took disciplinary action against the teacher for inappropriate conduct.
- Teachers who posted comments about their school suggesting they were not happy about certain policies and were not enthusiastic about their work. Again they faced disciplinary.
- A teacher who accidentally gave access to a pupil (through another Facebook friend) and faced a malicious and very upsetting campaign against her, but because she has technically given access to outsiders to her profile, also faced disciplinary action herself.

To avoid any of these issues yourself, you are advised to think of Facebook and any other personal social media site as public and **only write comments that you would be happy making to a parent or member of the public**. That means:

- All comments must be in support of the Academy/School MAT policy
- Any confidential policy items or issues must not be disclosed
- Any personal events or issues should only be posted if you would be happy speaking these publically to parents or pupils.
- You should not be friends with any pupil or former pupil if under 18 on Facebook or if they are still connected to the Academy via siblings or relatives, and should lock down your profile to ensure they cannot get access by accident (see details below).
- You should not add images of any students at the school without permission from the Principal
- You should not add images of the Academy that may be deemed inappropriate

Facebook: Managing your Profile

Facebook profiles for staff should be carefully managed to protect staff from possible problems which may arise from contacts from others on Facebook.

Here are some guidelines:

1. **Hide your profile from the search facility – otherwise anyone can search for you and send you messages**
2. **Filter your profile content so only your own friends can see your information. If you don't do this effectively friends of friends i.e. everyone can find a way to see everything on your profile.**
3. **Never have any current pupils or former pupils who still have connections with the Academy as friends on Facebook. If you already have any, remove them.**

You should be aware that Facebook is not 100% secure and anything you put on Facebook, regardless of your privacy settings, could leak into the public domain. So whatever you put on Facebook you should be happy for the world to see.

There have been discussions in the media about how Facebook can use any photos uploaded onto Facebook for advertising and other uses. This is all subject to privacy settings.

The link below is a BBC radio article that discusses this issue.

http://www.bbc.co.uk/programmes/p0121cpp

Below are other links that provide information for securing your social media sites

https://www.sophos.com/en-us/security-news-trends/best-practices/facebook.aspx

https://heimdalsecurity.com/blog/essential-guide-instagram/

http://www.tomsguide.com/us/lock-down-twitter-privacy-settings,news-18865.html

Sidney Stringer
Multi Academy Trust

Social Media Privacy Guidance

When using social media it is important to –

- **Know your schools policy and procedures**
- Think about your professional reputation and digital footprint
- Know the potential implications of poor social media use

If you have any questions or concerns following this please do not hesitate to contact a member of your leadership team or line manager for support.

Maintaining your professional reputation –

It is important that you keep in mind your online reputation even if you have appropriate security settings in place. Your online reputation could be created through your own posts, posts of others or even posts from people pretending to be you.

Your reputation should be important to you as the images and statuses posted could be seen by future employers, parents or students. Remember that anything posted to the web even if deleted may still exist.

Always think would I say that or do that in front of my colleagues/students?

Here is a brief guide to social media privacy on two of the most common websites Facebook and Twitter.

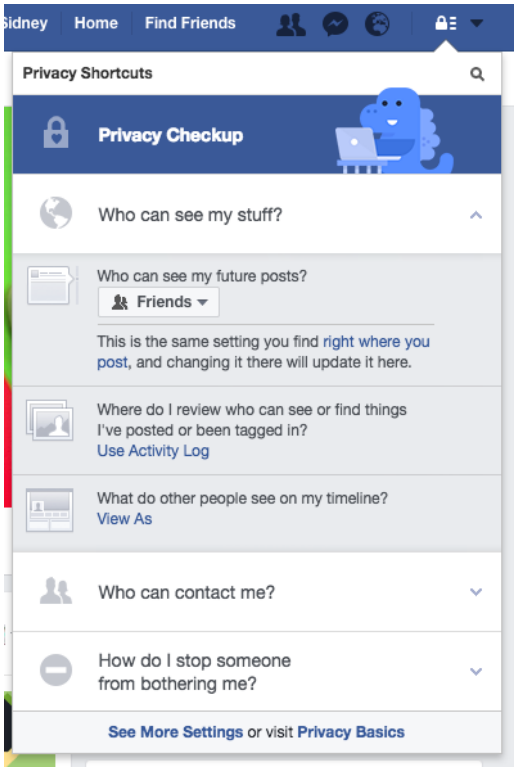
Contents:

Facebook
Twitter
FAQ

Sidney Stringer
Multi Academy Trust

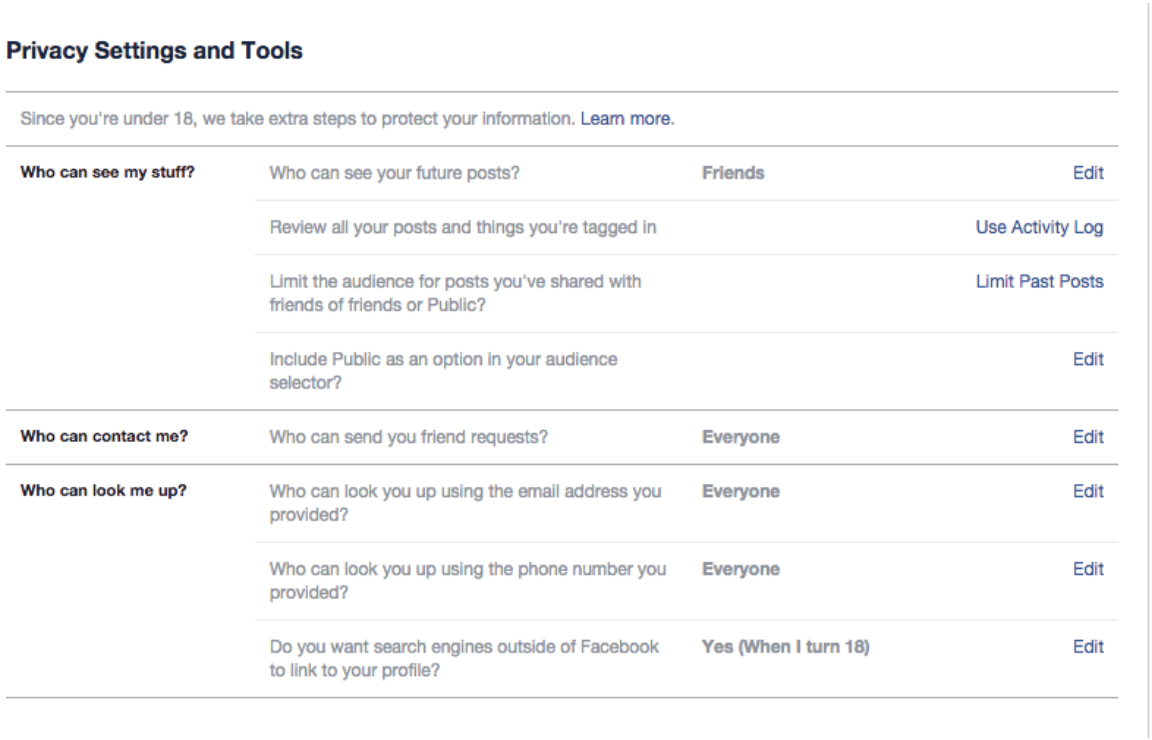
Facebook

Click the padlock on the top right of your profile homepage:



There are various settings in this section that you can change in order to lock your profile down.

By clicking See More Settings at the bottom you will see the options below:



Privacy Settings and Tools

Since you're under 18, we take extra steps to protect your information. Learn more.

Who can see my stuff?	Who can see your future posts?	**Friends**	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
	Include Public as an option in your audience selector?		Edit
Who can contact me?	Who can send you friend requests?	**Everyone**	Edit
Who can look me up?	Who can look you up using the email address you provided?	**Everyone**	Edit
	Who can look you up using the phone number you provided?	**Everyone**	Edit
	Do you want search engines outside of Facebook to link to your profile?	**Yes (When I turn 18)**	Edit

Ideally you do not want your posts set to Public. Clicking on the Limit Past Posts option will lock down previous posts that may have been public at the time.

Another key setting is the last one regarding search engines outside of Facebook. It is best to set this to No. This means that your profile cannot be found by searching on Google and other search engines.

The rest of the settings in the “Who can look me up?” Section should be ideally set to Friends or Nobody.

There is further help on Facebook regarding privacy and further explanations of all the settings:

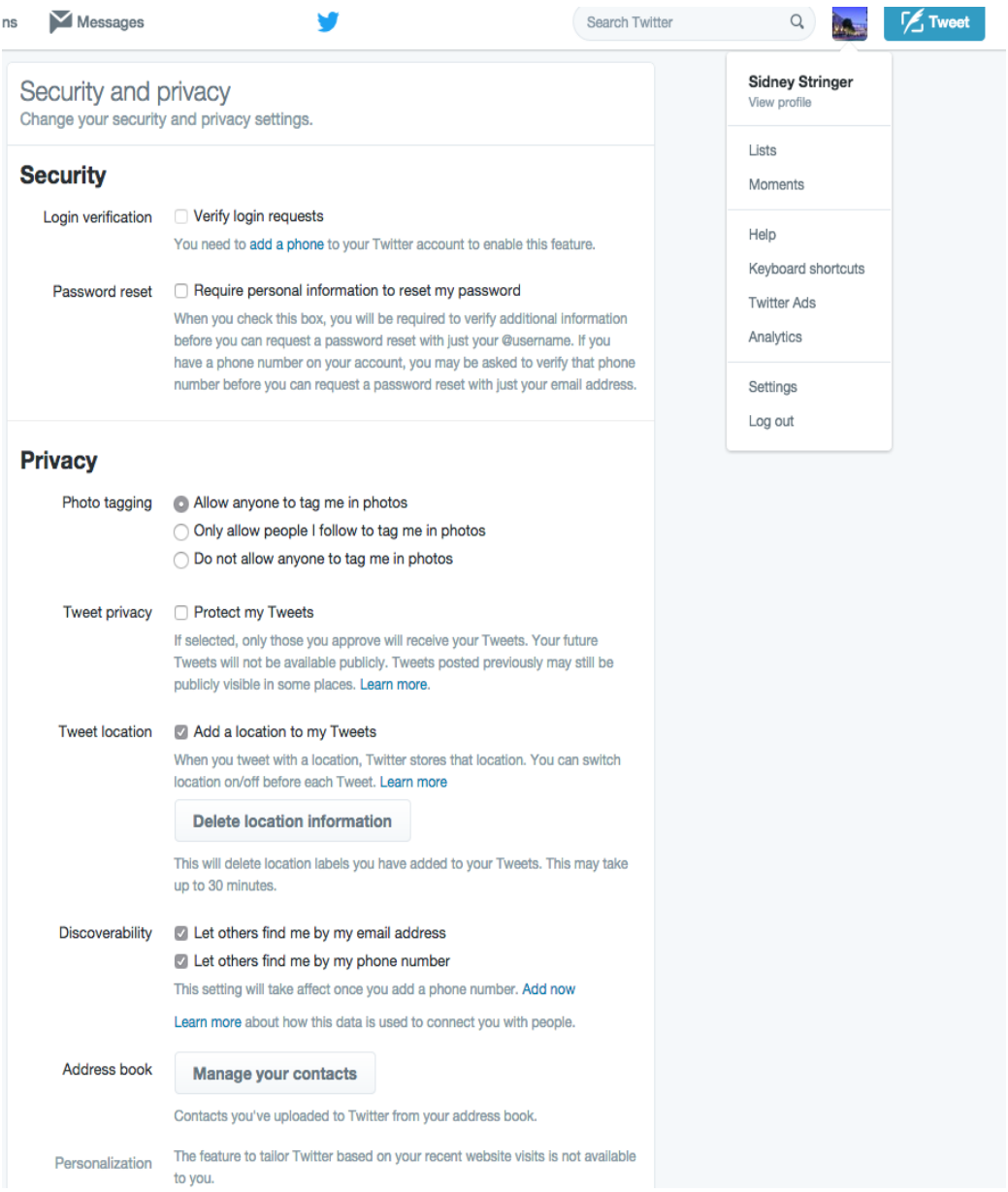
https://en-gb.facebook.com/help/325807937506242/

Sidney Stringer
Multi Academy Trust

Twitter

Twitter also has some privacy settings that you can access.

Click your profile photo on the top right from your Twitter homepage and click Settings. Then from the menu on the left click Security and privacy. You will see the options below:



The discoverability section is a key area, as it would be recommended to have both of those settings off. If you want your tweets to only be seen by people who follow you then you can tick the Protect my Tweets box.

There is an explanation and more help underneath the options on the page.

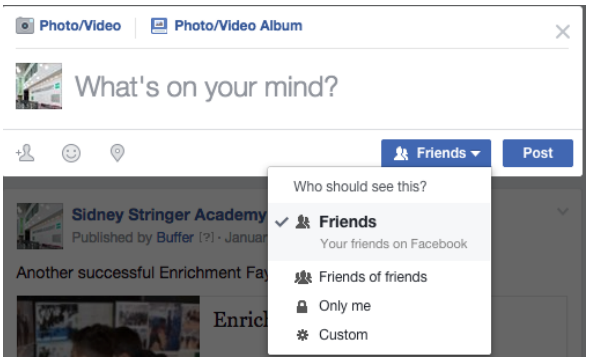
Sidney Stringer
Multi Academy Trust

FAQ

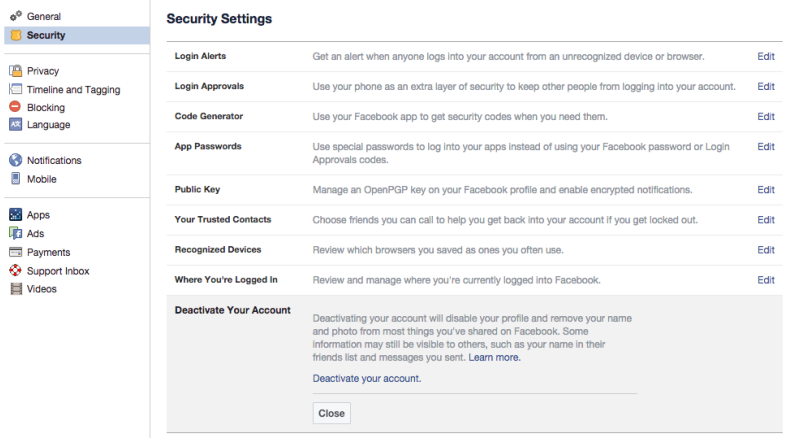
- Someone added me on Facebook from work but I think I already have him or her on my friends list?
    - Type their name in the search bar on Facebook and see if they come up as already being your friend. If so, the other profile could be a fake. Do not accept the friend request and inform the original person straight away or check with them in person.

- I don't want to add this person who has sent me a friend request because my Facebook profile is personal, what shall I do?
    - Choose to ignore the friend request and don't accept it. It isn't rude to do so!

- I don't mind having people from work on my Facebook, but I want to limit my posts, can I do that?
    - Yes. When posting, you can change who sees it and setup different groups by clicking the Custom option shown below:



- I've had enough of Facebook, how do I close my profile?
    - You can deactivate your Facebook by clicking Settings from the top right menu on your homepage and clicking the security section then using the option shown below:



    - You can do this for Twitter by going into the same Settings area as described earlier in this document and clicking Account in the left hand menu. There is a deactivate account option at the bottom of the page.

- Both websites have good help systems with much more detail on all of the features and options.