A teacher's guide to… staying safe on social media

Top ten tips

1. Think before you post

Are you happy with the content you are posting to be seen by a social audience, with parents, learners or governors able to see your posts or pictures? Most people may not consider who can actually see their posts, likes and comments. Think about the words and comments used, could they be misinterpreted? Could they be offensive?

2. Use the privacy settings

Make sure your privacy settings are set correctly. Ensure your albums, likes and comments are shared with those you intended to share with and are not for public viewing. There are checklists for Facebook, Twitter, Snapchat and Instagram that will help you with this.

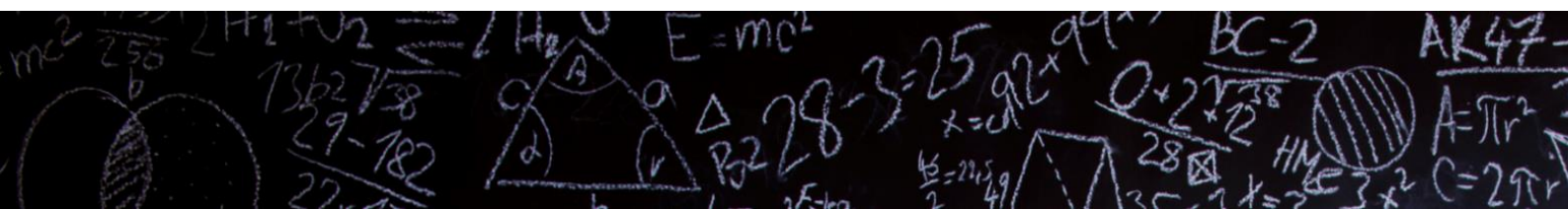
3. Be aware of your digital footprint

Search for yourself with a popular search engine to find out how others view you and your profiles. Ask a friend to look at how your profile appears to others or use the 'View As' function on your Facebook profile. This enables you to see how your profile appears to the public or to a specific person. Delete previous accounts of now unused social media sites.

The UK Safer Internet Centre has advice and information for practitioners on managing your professional online reputation.

4. Use strong passwords

Ensure you have a strong password which includes a mix of uppercase, lowercase and characters. Try and change your password regularly and keep it private. Do not disclose your passwords to anyone.



5. Have a social media policy for your school

Ensure you have a policy at your school which covers acceptable social media use by learners, staff and parents. Be aware of your establishment's policies and familiarise yourself with what is expected of staff members and learners. A list of editable policies from the 360 safe Cymru online safety self-review tool for schools can be found on Hwb

6. Have a school policy on the use of mobile phones

An Acceptable use policy needs to be agreed on by the school with regards to personal use of mobiles. Staff should be advised not to use personal devices when

- Contacting learners or parents (via text)
- Storing images of learners at the school

The 360 safe Cymru tool has a mobile technologies template policy you can adapt and use.

7. Hide your Bluetooth and air-drop while in school

Should your mobile device be close to learners, ensure the phone is 'hidden' and the bluetooth or air-drop is not visible to everyone. This will protect your phone from potentially receiving images sent by learners.

8. Use school devices for work purposes only

Staff should be advised to use school devices for work purposes when off premises, and to not share the device with others in the home. Files and storage drives taken from school should be encrypted if working on personal or sensitive data.

9. Agree how and if to share images with colleagues

If going out on a work night out, decide as a group what are the expectations with regards to posting images and online tagging. Respect every individual's wishes should they not want their picture to be posted online.

10. Report issues to providers

Know how to report content or an issue to social media providers should one occur. These social media checklists give advice on reporting issues to Facebook, Twitter, Snapchat and Instagram.

For advice and support with social media issues relating to you, your school or young people you work with, you can contact the Professionals Online Safety Helpline at helpline@saferinternet.org.uk or by calling 03443814772.

Llywodraeth Cymru
Welsh Government

SWGfL