

Social Networking, Social Media and Email: protecting your professional reputation

Guidance at a glance

This guidance paper is relevant to all staff in all schools and colleges. It offers information and guidance when considering the safeguarding of staff in their use of social networking sites (SNS), such as Facebook, Twitter and Instagram, both at school and personally.

The open nature of the internet and social networking means that everyone – including senior leaders – should take active steps to protect themselves and their school or college by taking simple precautions.

Your professional reputation is part of your current and future career, therefore managing your online reputation is essential.

Anything you post online or send by email is potentially public and permanent, even if you subsequently delete posts and emails and if you use privacy settings.

ASCL strongly advises you do not accept friend or follow requests on your personal accounts from pupils, past or present, or from parents at your school or college. By accepting such requests you could make yourself vulnerable by sharing personal information or by having access to personal information about pupils. This could leave you open to allegations of inappropriate conduct, as well as exposure to unwanted contact.

This guidance covers the following areas:

- Section 1** Protecting your professional reputation
- Section 2** Privacy settings and password security
- Section 3** Managing content and reporting abuse
- Section 4** Further information

1 Protecting your professional reputation

Think carefully before posting information about your school, college, staff, pupils or parents – even if your account is private. Comments could be taken out of context and be damaging. The language you use is important as abrupt or inappropriate posts may lead to complaints.

On SNS, friends can re-post or comment on your posts which means others to whom you have not given access may view your comments.

Think about how you present yourself when you post images, when joining a group or ‘liking’ pages; these choices say something about you. An employer may reasonably believe that a recognisable member of staff putting an inappropriate post or image in the public domain will lower the reputation of the school or college and that could be a basis for disciplinary action. It is an implicit condition of employment that an employee owes a duty of loyalty to an employer. In addition, potential employers may also look online and you will want to consider whether your choices show you in the best light when applying for a job.

SNS are utilised by some schools, colleges and educators as a means of connecting with parents, governors and students, however, this is done via organisational or professional pages and accounts. Prior approval is also obtained from the senior leadership team, and it should be borne in mind that 13 is the minimum age requirement of most SNS.

2 Privacy settings and password security

When using social networking websites it is important that you are in control of who can see your account details and content, including photos, albums, posts, status updates and any personal information. Accounts for Twitter, Facebook and Instagram can be set to private by following these steps:

Twitter

- a) click ‘profile and settings’ cog icon at the top right of the Twitter homepage
- b) select ‘settings’
- c) select ‘security and privacy’ from the left-hand menu
- d) tick ‘protect my tweets’ check box
- e) click ‘save changes’

By selecting the ‘protect my tweets’ option you will be able to either accept or decline requests to follow you.

Facebook

Choosing the ‘friends only’ setting for every option enables a good degree of privacy. Amend your Facebook privacy settings as follows:

- a) click on ‘privacy’ padlock icon, at the top right of your wall
- b) review ‘who can see my stuff’, ‘who can contact me’, and ‘who can look me up’
- c) select ‘edit’ on the drop-down menu

Instagram

By default, anyone can view your profile and posts on Instagram. You can make your posts private so that only followers you approve can see them. If your posts are set to private, only your approved followers will see them in the Photos tab of Search and Explore or on hashtag or location pages. Posts can't be set to private from a desktop computer.

To set your posts to private from the Instagram app:

iPhone or Windows Phone

- a) Go to your profile by tapping 
- b) Tap 
- c) Turn on the Private Account setting

Android

- a) Go to your profile by tapping 
- b) Tap 
- c) Turn on the Private Account setting

Updates to your privacy settings are automatically stored and do not need to be saved manually. Furthermore, you can customise each option and limit the information certain people can see. It is always useful to use the 'view as' option, to check how your profile appears to others and that the information you want to remain private or for 'friends only' is not visible to everyone. If you are not entirely sure about how to use all the settings, treat all of the information that you post as being available to everyone and act accordingly.

Friend or foe

It is a good idea to remove any friends, or customise the privacy settings for current friends, if access to your personal activity could compromise your position.

Be careful about comments you post on your friends' walls; if their profile is not set to private, your posts will be visible to everyone. Sharing content with others means that it is out of your control.

It is important, regardless of which setting you use, to assume that every post you make could be made public, as friends' settings do not guarantee privacy.

Geo-location services

There are clear implications about making sensitive information public. If using this feature on SNS, consider making your location visible only to your friends. It is also possible to disable the feature by which someone else can 'check you into' a location within your privacy settings, enabling you to control what information is shared.

Password and security

- Always use a strong password that contains a combination of upper and lower case letters and numbers and ensure that it is at least six characters long.
- Do not select the 'remember this password' option when logging on to a shared computer or device as others may later be able to access it.
- Log out after you have finished online to ensure the next user can't access your account.
- Always set a PIN or passcode on your mobile or tablet so access to your account is protected if you lose it.
- Keep anti-virus software up-to-date.

4 | Social Networking, Social Media and Email: protecting your professional reputation

Robust security settings could prevent hacking. Further, if an employee has kept up a reasonable degree of security and if the hacker clearly had to get through numerous barriers then the exposure of material could be excusable as there was a reasonable expectation of privacy. However, if confidential information that should have remained within the organisation has been revealed, the fact the leak has been exposed is irrelevant.

3 Managing content and reporting abuse

Search your name regularly online to monitor any content about yourself. This enables you to see what others can view and provides an opportunity for you to delete anything that may compromise your reputation. Be aware of what monitoring, if any, is carried out by the school or college.

Other individuals can post images on their profile in which you are named, so think about any photos you appear in. On Facebook you can 'untag' yourself from a photo. If you do find inappropriate references to you or images of you posted by a friend online, you should contact them and ask for that content be removed. Alternatively, report directly to Facebook to request its removal, although it will be Facebook's judgement as to whether it remains online.

In 2014 a European ruling against Google stated that the search giant must delete "inadequate, irrelevant or no longer relevant data" from its search results when requested. In theory, Google must remove links to personal information that is not relevant or in the public interest. However, the reality is that requests will still have to go through the courts resulting in a complicated battle. The information will still be available on the web, it won't be visible through a Google search.

Using email

All emails sent from a school or college account should be regarded as public, especially as a 'data subject access' request could be made under the Data Protection Act. Emails should always be in professional language and appropriate to being an employee. It should also be noted that where a private email account is used for issues associated with work, it has in some cases been deemed as a work account and therefore also subject to the rules of professional language and conduct.

In short, do not send an email that you would not be happy for your employer or a colleague to read.

Online harassment

Sometimes remarks aimed at an individual or the school or college go beyond inappropriate and become offensive and abusive. The best option is not to draw attention to these or escalate the issue; when ignored, the offended party may give up and the remarks end up being seen by only a handful of disgruntled individuals. However, if this continues it can become harassment.

There is a duty of care on the part of your employer to protect you from harassment. If they fail in this duty and you suffer harm they could be legally liable. Your first course of action is to contact the service provider to delete the offending remarks or close down the website. If this is not successful, ASCL considers it appropriate for the employer, rather than you, to take legal action to tackle the issue (or make use of the employer's legal advisers, for example the LA or retained lawyers), both because the employer should be protecting its employees from harassment and a slur on an employee is also a slur on the employer.

If the comments are offensive and sufficiently frequent they can be deemed as harassment in the criminal sense and should be reported to the police.

Unfortunately, it is difficult to make a legal case for defamation. For a statement to be defamatory it must tend to lower the claimant in the estimation of right-thinking members of society generally. A statement that amounts to an insult or is vulgar abuse is not defamatory. This is because the words do not convey a defamatory meaning to those who heard them (simple abuse is unlikely to cause real damage to a reputation).

Before you decide how you wish to proceed, consider that minimising any publicity will be a factor in your decision making.

School and college policies

Schools and colleges should have a detailed policy about the use of information communication technology, including social media. ASCL strongly advises that this policy states staff should not make contact with students through staff personal emails, by text on their personal phones or on social media sites. ASCL is seeing an increase in cases where behaviour of staff is either taken out of context or could be construed as questionable. Having a blanket ban on personal and private communication protects both staff and pupils.

Your school or college policy should also include specific guidance on the use of SNS. If the school or college encourages the positive use of SNS as part of the educational process then it should provide clear guidance on what is considered appropriate contact with students. Again, having a clear policy in place will help staff and pupils to keep within reasonable boundaries.

4 Further information

Support from ASCL

If you are facing disciplinary action because of something you have posted online or find yourself the victim of abusive online posts and cannot resolve the matter directly with the online service provider, please contact ASCL Hotline on 0116 2991122 or email hotline@ascl.org.uk

Guidance papers

Guidance paper: *An exploratory evaluation framework – safety and safeguarding, equalities, British values, the curriculum and governance*

<http://www.ascl.org.uk/help-and-advice/guidance-papers/ascl-guidance-paper-an-exploratory-evaluation-framework-safety-safeguarding-and-radicalisation.html>

Guidance paper: *Statutory duties related to safety and safeguarding, equalities, British values, the curriculum and governance*

<http://www.ascl.org.uk/help-and-advice/guidance-papers/ascl-guidance-paper-statutory-duties-related-to-safety-safeguarding-and-radicalisation.html>

ASCL's *Leader* magazine:

Social Media: Enjoy, engage or avoid? (July 2018)

http://www.leadermagazine.co.uk/articles/social_media_enjoy_engage_or_avoid/

Click, connect... take care (May 2017) www.leadermagazine.co.uk/articles/click_connect_take_care/

Extreme Measures (June 2015) www.leadermagazine.co.uk/articles/extreme_measures/

For more information about safety on the internet please see the following:

Young people and social networking sites – a guide for parents, carers and teachers

www.childnet.com/downloads/blog_safety.pdf

Facebook safety advice for educators www.facebook.com/help/441374602560317/

Information on Safer Internet Day www.saferinternetday.org/web/teachtoday/home

Resources from Childnet including a Social Networking Guide for Teachers

www.childnet.com/resources/kia/

UK Safer Internet Centre:

Resources for teachers and professionals

www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals

360 degree online safety tool <https://360safe.org.uk/Overview>

Online safety policy templates

<https://swgfl.org.uk/products-services/online-safety/resources/online-safety-policy-templates/>

How social media is used to encourage travel to Syria and Iraq – briefing note for schools
(DfE, July 2015)

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

