ASCL Association of School and College Leaders

GUIDANCE PAPER 117

Social Networking and Social Media – Guidance for Members

1 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 some simple precautions. The information below offers some thoughts as to what to do to safeguard yourself as well as other staff, and to avoid compromising your professional position.

Protect your professional reputation

2 Your professional reputation is part of your current and future career so managing your online reputation is essential. **Anything that you post online is potentially public and permanent even if you have used privacy settings on your account.** On social media friends can repost or comment on your posts which means others to whom you have not given access may view your comments.

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

4 Think carefully as to how you present yourself when you post images or 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.

Choose your friends carefully

5 Think carefully about whom you are friends with online and which friends can access what information.

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

Privacy settings

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

Click on the 'settings and help' cog icon, found on the top right of the Twitter homepage > select 'settings' > select 'security and privacy' > tick the 'protect my tweets' check box > click 'save changes'

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

8 For Facebook, choosing the 'Friends only' setting for every option enables you to achieve a good degree of privacy. Amend your Facebook privacy settings by following these steps:

Click on the 'privacy settings' padlock icon, found on the top right of your wall > select either 'who can see my stuff' or 'who can contact me' > select 'friends' on the drop-down menu

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 that 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.

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

10 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 could mean that you lose control of it; for example, friends could pass on your information.

11 Always use a strong password that contains a combination of upper and lowercase letters, and numbers and ensure that it is at least six characters long. Get in the habit of logging out after you have finished online. Not logging out means the next user can access your social networking account. 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. On your mobile phone always set a PIN or passcode, so if you lose or mislay it, access to your account is still protected.

12 Ensuring that you have robust security settings on your social networking accounts could prevent them from being hacked. If an employee has kept up a reasonable degree of security and if the hacker clearly had to get through serious barriers, then the exposure of material could be excusable; there was a reasonable expectation of privacy. However, if confidential information that should have remained within the organisation has been revealed, the fact that the leak has been exposed is irrelevant.

Manage what others post about you online

13 Search your name regularly online to monitor any content about yourself. This enables you to see what others can 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.

14 Other people could 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 and/or images of you posted by a friend online you should contact them and ask that the content be removed. Alternatively, you could go directly to Facebook to request that it be removed, although it will be Facebook's judgement as to whether they should be taken down or not.

15 In 2014 there was a European ruling against Google that the search giant must delete "inadequate, irrelevant or no longer relevant data" from its search results when requested. In theory this means that Google will need to 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 and could take a complicated battle to do so. The fact remains that the information will still be available on the web, it just won't be visible through a Google search.

Using email

16 The principles covered here apply to emails as well. 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, to be safe, do not send a private email that you would not be happy for your employer or a colleague to read.

Online harassment

17 Sometimes remarks aimed at an individual or the school/college go beyond inappropriate and become offensive and abusive. The best option is often not to draw attention to these or escalate the issue, as 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.

18 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 have the offending remarks deleted or website closed down. If this is not successful, ASCL would consider it appropriate for the employer, rather than you yourself, to take legal action (or make use of the employer's legal advisers, for example the LA or retained lawyers) to tackle the issue - both because the employer should be protecting its employees from harassment and because such a slur on an employee is also a slur on the employer.

19 Another possibility is to approach the police. If the comments are offensive and frequent enough it might mean that they can be counted as harassment in the criminal sense.

20 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 mere 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).

21 Before you make a decision as to how you wish to proceed, take into consideration that you will wish to minimise any publicity and this will be a factor in your decision-making.

School and college policies

22 Schools and colleges should have a detailed policy about the use of information communication technology, including social media. ASCL strongly advises that this state that 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 more cases of behaviour by staff which is either taken out of context or could be construed as questionable. Having a blanket ban on personal, private communication protects both staff and pupils.

23 Your school or college policy should also include specific guidance on the use of social networking sites. If the school/college encourages the positive use of social networking sites 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.

Support from ASCL

24 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 the ASCL hotline for advice on 0116 2991122 or email hotline@ascl.org.uk

Further information

25 For more information about safety on the internet, please see the following articles from ASCL's Leader magazine:

- School case studies **www.leadermagazine.co.uk/articles/digital_dangers/**
- Anti-Social Media **www.leadermagazine.co.uk/articles/antisocial_media/**

The following websites may also be helpful:

- 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/**
- Resources from the UK Safer Internet Centre **www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals**

Association of School and College Leaders

GUIDANCE PAPER 117

Association of School and College Leaders, 130 Regent Road, Leicester LE1 7PG
Tel: 0116 299 1122   Fax: 0116 299 1123   Email: info@ascl.org.uk

£2

August 2014

www.ascl.org.uk