SOCIAL MEDIA GUIDANCE FOR NUT ASSOCIATIONS/DIVISIONS (AND FOR DISSEMINATION TO NUT REPRESENTATIVES AS APPROPRIATE)

APRIL 2012

Public Facing

Your Twitter or Facebook page is effectively your website, findable via Google. It naturally follows that, if your account is visible to all and you are a representative of the NUT, then you must behave accordingly. You will be assumed to represent the NUT if the personal information description next to your name includes a reference to being an officer or representative of the Union or uses the NUT initials. Using the phrase "tweeting in a personal capacity" cannot really co-exist with that. Journalists will still have the inclination to consider you fair game.

Whether you are operating a social networking account yourself or as an NUT association/division officer or representative, you should:

- not post information and photos about yourself or school-related matters publicly that you would not want employers, colleagues, pupils or parents to see;
- keep passwords secret and protect access to accounts;
- not befriend pupils or other members of the school community on social networking sites (you should consider carefully the implications of befriending parents or ex-pupils and let school management know if you decide to do this).

Reputational Risk

If local associations and divisions or school representatives make unwise postings on accounts that are clearly identifiable with their association or division or school group and display the NUT name or logo, then there is an obvious reputational risk to the NUT. You risk harming your own individual reputation too. Teachers are always under a professional duty to demonstrate honesty and integrity and uphold public trust and confidence in the teaching profession. The informality of social media and the speed of comment and discussion create a constant risk of reputational harm if unwise comments are made.

Language

Insulting, derogatory and discriminatory language have no place on the Twitter account of an NUT representative. Your NUT Twitter feed is not the place to write personal or derogatory remarks about any person or organisation. All comments must remain professional. This is not your personal account and it must be remembered that an NUT association/division or NUT school group Twitter account represents all members, not just yourself.

Defamation

The law of defamation allows persons who consider that their reputation has been harmed by statements made by others to sue for compensation. Defamation law certainly applies to statements made on social media sites. You can even be at risk if you pass on/retweet/share defamatory statements made by others. Defamation law is complex. The essential message is 'do not make derogatory personal comments about other individuals'.

No Such Thing as Privacy

There is a debate about whether or not information is ever deleted from social media sites. Both Twitter and Facebook say that their accounts can be permanently deleted. You need to be aware that even though you may think you are only using social media for 'personal' use, you may be building up a record about your views and activities that is accessible to a much wider audience than you intended. Increasingly employers are carrying out internet searches into prospective employees.

Clarity

When tweeting remember that what might be obvious to you is not necessarily obvious to anyone else. It is, therefore, important to make sure that the tweet makes sense to someone who is coming to the comment for the first time. For instance, a comment on a council meeting will be incomprehensible to someone who was not there if relevant details or a link to a fuller statement is not included in the tweet. If possible, please get another colleague to check your tweet for obvious spelling mistakes and any factual information that is incorrect.

Confidentiality

If you are contacted in public by a member, via social media, make a judgement on when the conversation should become private. To make the conversation private, simply ask them to send you a private message or provide an email address to which they can write. Their privacy, particularly about issues to do with their workplace, must be paramount. Employers can and do use in disciplinary proceedings material obtained from social media. Those, such as teacher governors, must take particular care not to divulge information obtained from carrying out their responsibilities.

Security

In terms of security, the risks involved when using social media tend to be similar to the risks involved in using computers, technology and the internet in general. Users of Twitter, Facebook, etc., are equally vulnerable to spam, viruses, malware (dubious apps), targeted attacks, etc. The basic advice is:

- do not open attachments unless you are expecting them and they are from a known and trusted source;

- be wary of clicking on URLs (web links) which are from untrusted sources;

- keep up-to-date with security updates and software upgrades as these often include protection from current viruses.

At the start of your social media journey, you would have created a login and password. When accessing social media sites on a handheld device, e.g., iPhone, blackberry, etc., we tend to enter this information once, creating an always open connection to each site. If the device has no other password protection and falls into the wrong hands, these accounts can be accessed and used until you change each site's password.

To protect your accounts, ensure all devices (iPhone, blackberry, android phones, playbook, iPads and other hand held devices) require a login to open the device before these and other functions can be accessed. This should provide some protection until you can change passwords.

Report lost devices immediately. Change your passwords as soon as possible and report to the social media site any evidence that your account has been compromised. With so much personal information about individuals on the web, whether you are an avid social networker or not, it is much easier today for someone to have a good guess at the passwords for any of your accounts. If your password is compromised, your social networking sites could be hacked and used so it is best to use passwords that are unrelated to you. Change passwords regularly or use strong passwords mixing letters, numbers and characters: e.g., Twitter = +w1TT3r.

Check your social networking accounts regularly to ensure that they have not been hacked and, if they have, change your passwords straight away and report the matter as you may need to create a new account. Be careful of the sites you choose to sign-up to via your social media sites, e.g., if your FB account is for family/friends, do not use it to sign up to a work/professional related site or service.