# Social media guidelines

Process

| Policy / Policy Update Presented by/on behalf of: | Associate Principal | 28th April 2016 |
|---|---|---|
| Presented to: | Behaviour, Safety & Ethos Portfolio Team | Agreed 28th April 2016 |
| Approved/Ratified: | Academy Board | Approved/Ratified 16th June 2016 |

**Date of policy/latest review:  Sept 17 – no amendments**
**Next review:    Sept 18**

**Information in this booklet has been adapted from e-safety advisor.com**

**Introduction - Twitter**

Twitter is a great Social Networking service that allows you to send chunks of bitesize information in 140 characters or less. Known as a "microblogging" service it was conceived in much the same way as Facebook; to share information with a small group of people.

Created by Jack Dorsey he defined the microblogging service as, "a short burst of inconsequential information." His first tweet sent on March 21st 2006 was, "just setting up my twttr." Twttr was the original name.

Since then Twitter has grown massively. In 2012 the service is close to 150 million users tweeting over 340 million tweets daily and over 1.6 billion search queries. *(source: Wikipedia)*

The ways in which Twitter is being used are immense; for example:

- As a teaching and learning tool for working together (collaborative).
- To communicate with your friends and family overseas.
- To follow your favourite bands, musicians and other celebrities.
- As an emergency communication system.
- To make things more engaging, for example TV shows and conferences.
- News networks and as a sales/marketing tool

User agreement

If you are intending to use twitter with pupils it is worth using the following guide to ensure good safeguarding at the National Academy with pupils. Pupils should have the opportunity to discuss, consider and understand the agreement before they start using twitter with staff members.

Liability

National Academy holds the liability as a result of facilitating this service; therefore it is essential that basic safeguards are adhered to.

Benefits for pupils

Rather than sheltering pupils from the potential dangers of using any social media (not just twitter) it is important to educate them in safe use. There are risks, but using a few simple rules, pupils (and staff) can protect themselves and stay safe online.

# TWITTER – Security Settings and Safe Use

## Pupils MUST be 13 years or over to use Twitter

Twitter is a great microblogging service. By remembering some simple tips staff and pupils will remain safe and secure and will be able to enjoy the benefits of using this service.

## Remember

- Twitter is a social networking service; all your tweets can be seen or searched by anybody.

- Protecting your account prevents people from following you automatically.

- It also stops people you haven't approved reading or searching your tweets. If you wish to protect your account you can do so in the Settings.

- Use a strong password to stop your account from being hacked and change it regularly.

## A Guide to Safe Use for Young People

1. Don't post any personal information such as your age, where you live, mobile phone number. If you have to, use a Direct Message.

2. It is very easy to tweet something in the heat of the moment and regret it later. Never post anything that could upset somebody else.

3. If you find something upsetting don't reply; tell an adult you trust. If it carries on "block" the sender.

4. Remember that not everybody is who they say they are.

5. If somebody asks you to meet them in the real world, tell your parents or an adult.

IF YOU ARE BEING BULLIED OR HARASSED TELL AN ADULT OR YOUR TEACHER STRAIGHT AWAY

## Social Networking hints and tips

Social networking sites are brilliant ways to stay in touch with friends and share photographs, comments or even play online applications such as chess or word games. However, they are also designed to enable advertisers to target you and entice you into buying goods and services based on the 'profile' information you reveal. Be web savvy!

- Social networking sites, such as Facebook, have a range of privacy settings. These are often set-up to 'expose' your details to anyone. When 'open' anyone could find you through a search of the networking site or even through a Google search. So, it is important to change your settings to "Just Friends" so that your details, photographs etc, can only be seen by your invited friends.

- Have a neutral picture of yourself as your profile image. Don't post embarrassing material.

- You do not need to accept friendship requests. Reject or ignore unless you know the person or want to accept them. Be prepared that you may be bombarded with friendship requests or 'suggestions' from people you do not know.

- Choose your social networking friends carefully and ask about their privacy controls.

- Do not accept 'friendship requests' on social networking or messaging sites from students, pupils or young people (or their parents) that you work with. Remember ex-pupils may still have friends at your school.

- Exercise caution – for example in Facebook if you write on a friends 'wall' all their friends can see your comment – even if they are not your friend.

- There is a separate privacy setting for Facebook groups & networks, you might have your profile set to private, but not for groups & networks. If you join a group or network everyone in the group or network will be able to see your profile.

- If you have younger family members on your social networking group who are friends with your students or pupils be aware that posts that you write will be visible to them.

- If you wish to set up a social networking site for a school project create a new user profile for this, do not use your own profile.

- If you or a friend are 'tagged' in an online photo album (Facebook, Flickr or similar) the whole photo album will be visible to their friends, your friends and anyone else tagged in the same album.

- You do not have to be friends with someone to be tagged in their photo album.

- If you are tagged in a photo you can remove the tag, but not the photo.
- Photo sharing web sites may not have privacy set as default.

- Your friends may take and post photos you are not happy about. You need to speak to them first, rather than contacting a web site. If you are over 18 the web site will only look into issues that contravene their terms and conditions.

- Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a 'web crawler' and it will always be there. Archives of web content are stored on sites like the WayBackMachine.

- Think about your internet use, adults are just as likely to get hooked on social networking, searching or games. Be aware of addictive behaviour!

- You will not be able to remove yourself completely from the Internet. 192.com has all the English electoral roles and for as little as £9.99 your personal information can easily be found by a stranger.

- Please be aware that any comments or images posted are permanent and could be searched for later in life.  This is particularly important for young children.


## Wider Internet hints and tips

- Never tell anyone your password.

- Be careful how you choose passwords, most are very predictable. It is easy to find personal details online that might give password clues. It is recommended that you include capital letters, lower case letters and numbers – avoid birthdates, names, pets, addresses etc. It is best to avoid any word found in a dictionary.

- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.

- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.

- Be careful when form filling online…., do you know who the data is for? Only answer 'required' questions, do not just give out information because you have been asked for it.

- Never verify banking details online.

- When you need to use a 'name' online consider what name you use. In a professional context you would probably use your full name, but in other contexts you may decide to use an alias to protect your identity. If so make sure it is appropriate.

- If you create a family tree and post it on the Internet, make sure your tree is set to private for anyone living or recently deceased (last 50 years). The information posted would be enough for someone to steal your identity and probably guess passwords and common security questions.

- If you get a phone call or an email from someone asking you to confirm personal details, (unless you are expecting the contact) do not give out any personal information.

- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name, sites cannot work from a hunch.
- Cookies are not necessarily a bad thing. They save your surfing information and speed-up access to sites. However, if someone else has been surfing 'adult content' on your computer, the stored cookies may mean you get 'adult pop-ups and adverts'.

- Use legal sites for downloading music, films etc., such as iTunes.

- File sharing sites are not illegal but sharing of copyright material is. Downloading of illegal music and film downloading also leaves you at a huge risk of viruses. Even if you subscribe to a file sharing web site, such as Limewire, it does not mean that your downloading becomes legal.

- You can get Internet access from many games consoles and some MP3 players. Games with multiplayer features are often labelled as 'net play'. This means that you are playing with strangers online – the risks here are the same as for social networking, chatrooms and messengers.

- Applications like Skype and iplayer need bandwidth and can slow down the internet, particularly if you use a 3G mobile stick. Full screen iplayer could use up your allocation and your service may be 'throttled' - meaning you can only do some basic text work, searching and emails, but picture and video will not be possible.

- When you log-into a web site, unless your computer is exclusive to you, don't tick boxes that say 'remember me'.

- Don't leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.

- Don't give your username and password to anyone such as to a supply teacher / temporary member of staff – make sure your school has a guest login for visiting staff.

- Your school or work laptop (or other equipment) should not be used by friends and family.

### Internet use for working with young people:

- Try to provide pupils with direct links embedded into 'pages' in a document, a learning platform 'room', or interactive whiteboard resource etc.

- If you do need to undertake Internet searches (including Internet image searches), rehearse before you use in class. Think about search terms. Even the most innocuous term can bring up adult material.

- Use child-friendly search engines like www.askkids.com with younger pupils. Older young people will use a variety of search engines at home, you are a role model for them in good use of a search engine. Look for opportunities to teach young people how to use search engines.

- When checking out web content make sure you are not displaying it on the interactive whiteboard or via a projector – research away from pupils.

- Watch YouTube (or any) videos before you use them in the classroom.

- If you use a YouTube (or any) videos, find out how to embed it using the 'Source' rather than a page link, as that exposes pupils to other content.

- If you cut and paste or save content from the Internet or other peoples files make sure you remove the hyperlinks embedded in the text, or attached to images.

- If you want to use a clip download it (if legal & copyright allows), it might not be there next time you look for it.

- If you use your own equipment in school (such as cameras or laptops), ensure senior leadership have given you permission and make sure that school files (photographs etc) are downloaded and stored in school, not at home.

- Do not take stored pupil photos or information home. If for any reason you need to ensure you have senior leadership's permission, and ensure it is on an encrypted device.

- Video Conferencing – you can be broadcasting without realising it, if you have VC in your classroom make sure it is switched off after use and that the camera is turned away from the class.

- You need to be a role model for copyright. Make sure you use multimedia resources appropriately, don't just 'grab stuff' off the Internet. Use the copyright images from the National Education Network (NEN) or other sites your school / LA has advised you of. There are limitations to showing DVDs in school, although it is safe to use film trailers. But, make sure you download the right version, as there are can be more than one film trailer, including trailers for 'adult versions' of blockbusters.


## Email hints and tips

- Keep all professional work and transactions completely separate from private. Create a web-based email account for private online business, such as online shopping and ensure you use your school / work email only for any professional communications.

- Create yourself a hotmail (or similar) account to use when searching for insurance quotes etc, when you are done either close the email account, or ignore it. Any junk mail generated will then not affect you.

- If you get an email from someone or a company that you have never heard of and it asks you to reply to unsubscribe, don't. By unsubscribing you will verify that you exist. Just ignore the email. If they carry on emailing use email rules to block the sender.

- If you get emails that offer you money making schemes (e.g. the 'Nigerian email'), Russian wives, pharmaceutical products and body part enhancement don't be upset, you have not been personally targeted, this is spam and junk mail.

- Webmail is useful but insecure, and your email address is easily passed on.

- If you get spam or junk mail it does not mean that someone has 'hacked' into your email; people get email addresses in different ways, it might be a software 'guess' – a programme generates lots of possible emails and sends out millions of emails knowing that statistically some of them will be real. Software also searches web sites for email addresses and harvests them.

- Only open Email attachments from trusted sources, you won't get a virus from the initial email text, but it may be contained in an attachment.

- If emails from friends or acquaintances start to become unsuitable – say something before you receive something really problematic.

- Don't give out private email addresses to students and pupils.

**Hints and Tips: YouTube**
- It is always better to review video clips before using them in class – otherwise you won't know if all the language and situations are appropriate or useful.
- If you must do a 'live' search, temporarily switch off the whiteboard. This is for at least two reasons; the search may return unexpected results, and students are also seeing the 'most popular', what's new and other un-moderated sections. However, EMBC will block most of the advertising content. Here is a screenshot of the usual entry page – occasionally the featured or 'trending' videos are inappropriate:-
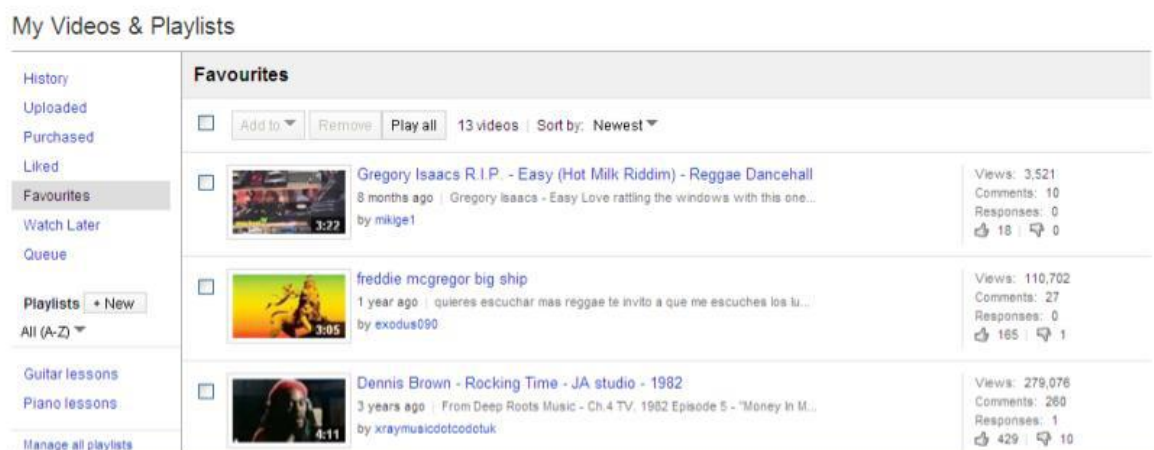


- **Solution**: Find the relevant video you need on your teacher machine having cut the signal to the IWB. When you have located it switch to 'full screen' mode and re-enable the whiteboard. This way the pupils will only see the video itself.
- You can avoid the general search page by saving videos to your own account, which is easy to set up. If you have a personal YouTube account don't use it for school –

create an account specifically for work, and ideally get approval from a senior colleague.

- The advantage is that you can store all your favourite teaching clips as you come across them and it will also suggest related content based on your recent searches which can be useful. However, a small amount of un-moderated content will still appear down the side on your homepage.
- **Solution**: Save video clips to your 'favourites' area. In this way you can avoid all adverts and other videos appearing – this is probably the best way to use YouTube with a live connection. Here is a screenshot of a favourites area:-



- It's always advisable to check that your chosen video runs on the machine you will be using. Sometimes computers will lack bits that enable them to play. (e.g. video 'codecs', browser plug-ins etc)
- Different machines can have different levels of internet access in schools. Check that you have internet access to what you need to use. Schools that have 'local control' of filtering can adjust access levels as required. For help please contact the local authority broadband officer - chris.hale@nottinghamcity.gov.uk

### Downloading videos for playing 'off-line'

- You can avoid problems with internet access, adverts and suspect content by downloading videos to your local computer
- Copy or 'rip' the videos to your own machine using software such as 'you-tuberipper' (www.you-tuberipper.net ) or Real Player. This means you can play them directly from your machine and not have to rely on internet speeds / connections.
- If you have video clips stored on learning platforms or in other locations, it's a good idea to copy it to your desktop before playing it, as it is more likely to play smoothly without 'stuttering'.