USING TECHNOLOGY SAFELY:

A checklist for using technology safely with young people in the classroom, at school or even at home.

Technology is a vital part of both young people's lives and an educators professional and personal life. The following checklists, along with the **'Social Networking guide for teachers and professionals'**, have been designed to ensure that you are able to face these challenges whether at school or at home.

At home

Managing your professional reputation

- **Google yourself** - review online content which relates to you and take steps to secure or remove any private or unwanted content.

- **Choose profile pictures wisely** - even with a private account the profile picture and bios are usually visible. So think carefully about what you share and what it might say/ reveal about you.

- **Think before you post** - be mindful of how pupils; parents; and employers may view you and your online content.

- **Act according to school policy** - schools have policies about anything which can cause harm or distress to others or brings the name of the school into disrepute, including content shared out of school hours.

Securing your content

- **Privacy settings** - setting these to private will allow you to control who can see the content you share. They can usually be found within the settings of the account. Although remember that content can easily be screenshotted and shared more publically.

- **Pin/passcode on devices** - always set devices up with a strong pin/passcode lock to ensure personal data and images are secure.

- **Strong passwords** - Make sure you use a mixture of lower and upper case letters, symbols and numbers within a password as this will make it stronger. Also remember to change them regularly and keep them to yourself.

- **Logging out** - always log out of online accounts when leaving a device in order to secure the content.

What to do if you are the target of cyberbullying

- **Don't retaliate/ respond** - this will often aggravate the situation further.

- **Keep the evidence** – screenshot or print out all content and keep a record of any incidences you are unable to capture content of.

- **Report** - You can report online content directly to the site as well as to your senior leadership team who should support you in handling cases of cyberbullying.

- **Seek advice** - this could either be through your senior leadership team or by contacting the **Professionals Online Safety Helpline** (POSH) who can support professionals with any online safety concerns, including cyberbullying. **0844 381 4772** or **helpline@saferinternet.org.uk**

Professionals Online Safety Helpline

In the classroom

Using technology and the Internet safely

- **Use school devices** - where possible try to use school devices which should already have appropriate filters applied at device level or across the school internet.

- **Set rules for use of personal devices** - If using personal devices is appropriate then set clear rules for use in class. This could include what apps to use or whether or not image taking would be appropriate for the activity.

- **Guide pupils to appropriate sites** - you may consider selecting sites for younger pupils or discussing with older ones what content they may be looking for when carrying out an online search.

- **Model good behaviour** - consider the pupil's privacy when sharing their images online. Regardless of whether you have obtained media consent, model best practice by asking their permission before posting an image of them online.

- **Act according to school policy** - schools will have Acceptable Use Policies (AUP) for all members of the school community. Familiarise yourself and your pupils with these rules frequently.

Handling young people viewing online content

- **Check online content first** - always make an effort to check online content first either by fully exploring any webpages you may show in class or by watching videos in their entirety.

- **Check search results first**– if you are going to search for content with the class, perform a 'dry run' first to ensure the content is appropriate. Sometimes the most innocent of searches can return unexpected content.

- **Capture content** - you may wish to save content or take screen shots to ensure adverts/ comments haven't changed since you last checked.

- **Apply safety modes** - where available use the settings of the site/ app to filter the content they search for. Google offer a 'safe search' setting which can be found in the top right corner and YouTube offer a 'safety mode' which can be found at the bottom of the screen or within the settings of the app.

- **Check school policy** - be clear on your school's policy for viewing inappropriate content in class and share this with the pupils. Ensure that they are aware of the different policies and sanctions, eg if it is viewed on purpose or by accident

Incorporating online safety into the curriculum

- **Whole school approach** - online safety messages should be embedded in all areas of the curriculum as many subjects now frequently use technology or ask pupils to conduct online searches. Ensure pupils are reminded of online safety messages whenever using technology and the internet.

- **Use a range of resources/ teaching methods** - there are a wealth of online resources to support you in delivering online safety messages in a range of ways. You may wish to use our 'Online Safety in the Computing Curriculum' guide to resources for suggestions—**www.childnet.com/resources/online-safety-and-computing**

- **Stay up-to-date** - technology and online content can change rapidly year on year. Ensure you are teaching about the current risks and trends by researching or speaking to pupils. You could also sign up to our weekly newsletter by visiting our website.

- **Give advice or routes to get help** - ensure pupils know what to do if something goes wrong online. This could include speaking to an adult, saving evidence, reporting content or contacting a helpline for support.

In School

Best practice for using technology and the internet

- **Review policy regularly** - ensure the school's policy and AUP is up to date and has been shared/ communicated with all members of the school community.

- **What to do if...** - consider how your school will put your policy into practice. Outline how staff should react in different situations, eg where a pupil has misused technology and the internet on purpose or by accident.

- **Review school procedures** - as online issues evolve it is important to review school procedures and ensure teaching and responding procedures are effective. You may wish to use the free 360° safe online self review tool - **360safe.org.uk.**

- **Use appropriate methods of contact** - only contact pupils and their families through school channels, eg a school social networking page

- **Secure school devices** - ensure devices have up to date firewalls and safety modes in place and are secured with passcodes.

- **Apply appropriate filtering and monitoring** - schools are required to establish appropriate levels of filtering. Find out more **www.saferinternet.org.uk/appropriate-filtering-and-monitoring.**

Using technology safely and social media safely offsite

- **Use school devices** - in order to secure images and contact details it is best to use school devices for communication with young people and families or to take images.

- **Avoid sharing personal details**– most schools specify that staff should not give out personal mobile numbers or email addresses to pupils or parents as these details could easily be shared with others.

- **Review school policies and AUP beforehand** - schools will have clear policies on the use of technology and social media and this should include offsite usage as well. Familiarise yourself and the pupils with this. This may include appropriate communication with others, taking/ sharing images and sharing location details online.

- **Consider online risk** - where necessary remember to include possible online risks when completing risk assessment forms.

- **Set rules for personal devices** - pupils may bring personal devices on trips so it is important to communicate whether this is allowed and the appropriate rules for use of a personal device during the school trip.

Using images of children and young people

- **Obtain consent** - before videoing or photographing pupils ensure you are clear about the school's policy and that parents and carers have completed relevant consent forms.

- **Use school devices** - it is advisable to only use school devices when capturing images or videos of students as it is then stored on that device.

- **Consider where it will be stored and how long for** - when saving a file ensure this is on a secure school network or encrypted USB and deleted when no longer required.

- **No names** - it is best practice not to share the image with the child's full name in order to safeguard their welfare.

- **Consider appropriateness of the image before sharing** - not all images which may be taken are appropriate to be shared online. Caution may be needed in taking photos at sporting events, for example during swimming lessons or events. It is also best practice to ask the child before sharing an image in a public space as it may embarrass of upset them.

Co-financed by the Connecting Europe Facility of the European Union

SOCIAL MEDIA

A guide for teachers and professionals

INTRODUCTION

Social media services like Twitter, Facebook and WhatsApp have very quickly become a part of our lives; changing the way we keep in touch with friends and family as well as the way we share ideas and get information. This guide is designed to support your personal and professional use of these services in order to keep pupils, yourself and your job safe.

NOTE: For guidance on setting up an account for your department or school and managing your schools online read LGfL's Online Reputation Management for Schools -

onlinerep.lgfl.net

LONDON GRID FOR LEARNING UK Safer Internet Centre

Managing your school's online reputation – *If you don't, someone else will*

PRIVACY SETTINGS

Whilst it is important to remember to think carefully about the things you share online - because they may be shared by others - social media sites have privacy settings and safety features to help you manage who can contact you and see the things you share online.

Should I make all my social media accounts private?

The key is to determine what you want to use that particular social media account for and then decide:

PERSONAL USE

If you are using social media in your personal life you should make the account private. In most cases, if an account is private all someone will be able to see is the account name and profile picture.

- □ Make account private
- □ Use a different name or variation of your name
- □ Use an appropriate headshot or picture

PROFESSIONAL USE

If you are using social media to network, share your ideas, showcase achievements and discuss issues you can make your account public. If you are public, remember that anyone can see what you post.

- □ Account could be public or private
- □ Use your name and/or subject eg MsSmithICT
- □ Use an appropriate headshot or picture

What should I use privacy settings for?

Securing my personal information

Social media sites are all about sharing and this could include some of your personal information. Use the settings to control how much appears on your profile and who can see it. For advice on security for your accounts and devices please see our Using Technology Safely Checklist.

Customising who I share posts with

Some sites allow you to create groups or you can even select specific friends to share that particular post with.

Controlling who can contact me and make friend requests

If your account is public this usually also means that any user can add you or even just view the posts you are sharing. Locking your account down to private will mean that you will be sent a request when someone wishes to follow you which you can accept, decline or ignore.

Keeping your location private

Social networks allow you to tag your location to your posts (ex. on holiday or at a restaurant) but it is important to remember that your location is key personal information. You do not have to add your location to posts and you can also prevent social media from accessing your location at all through the privacy, location or app settings.

Be aware that if you are on a **school** trip with pupils you should not share location information to ensure their safety.

Tagging

Your name could be tagged in a photo or on a post you would be interested in. This is great for finding things quickly but ultimately this can lead to these posts being seen by a far wider audience. You can use the settings to make sure you have to approve tags or are notified whenever somebody tags you.

For more detailed information on **privacy settings** and how to set them up for the main social media sites visit: www.saferinternet.org.uk/safety-tools

! Scenario

A pupil has found holiday photos of you on a social media account and shared them with their friends. Here is our advice...

Evidence Note down what happened and who is involved. Screenshot or take a photo of anything relevant.

Tell your school It is best to let your school know as soon as possible so that they can talk to the pupils involved and to prepare them if there are any complaints.

Find the source(s) Find the photos and make them private or remove them if you wish. If hosted on a friend's account ask them to take them down. Consider making all your accounts private and removing any photos that could impact your professional reputation

Seek further help Call the **Professionals Online Safety Helpline (POSH)** for any further help and advice on 0844 381 4772 or email: helpline@saferinternet.org.uk

MANAGING YOUR PROFESSIONAL REPUTATION

Search and search again

The best way to find out your online reputation and **test your privacy settings** is to search for yourself regularly on a search engine.
If you do find any negative or upsetting posts that will impact your professional reputation then save the evidence by taking a photo or screenshot and tell your school. Do not reply or comment on the post.

Instead use the reporting procedures of the site(s) involved and contact the **Professionals Online Safety Helpline** for advice. If you find an account that has been set up in your name then you should also tell your school and report to the social media site it is on. When reporting make sure you add as much information as possible.

For more help and guidance on reporting please visit:
www.childnet.com/resources/how-to-make-a-report

TOP TIP
When searching, use your name and location first then check variations of your name and even try nicknames.

IMPORTANT

Social media sites often update their privacy settings and may add new features. Revisit your settings on a regular basis to check.

Unsure about how to use the settings available? Treat all information that you post as being public and then act accordingly.

Think before you post

Is that photo appropriate? Could that joke be seen as offensive? Should you respond to that comment you did not agree with? Be mindful when sharing pictures or posts or liking content online which could bring your reputation or that of your school into disrepute. Hashtags can link your content to other content with the same hashtag. **#BeAware**

What about the things my friends and family share? How do I talk to them?

With social media you are only as private as your most public friend. You may have a friend who loves to share all aspects of their life online and that affects you. It is worth talking to them about privacy settings and being mindful of your professional reputation.

INAPPROPRIATE CONTENT ON SOCIAL MEDIA INVOLVING YOUNG PEOPLE FROM MY SCHOOL

The key message here is to tell your school. Certain issues like cyberbullying and self-harming would be a matter for your school's Designated Safeguarding Lead. If you were to see this or inappropriate comments about the school or staff you should take screenshots or photos as evidence and inform those responsible for behaviour in your school. If you see a young child on social media that are putting themselves at risk you should also report this to your school.

If the content which you see online may be an example of sexting then we recommend you refer this immediately to your Designated Safeguarding Lead. For more information on handling incidents of sexting please refer to the UKCCIS Sexting Guidance for Schools and Colleges.

RESPONDING TO FRIEND OR FOLLOWER REQUESTS FROM PUPILS

Current pupils

We recommend declining the request and most school policies will state that you should not accept friend requests from current pupils. If you are receiving frequent requests from the same pupils then speak with your Senior Leadership Team or consider blocking the pupils to prevent further requests.

If pupils are under the age of 13 (the age that most of the popular social media companies have to legally comply with) it is worth asking the young person if their parents or carers know they are using social media and checking they know how to keep themselves safe.

What about former pupils?

Pupils from a previous school, those who have moved schools or who are now adults may not be covered by your school's policy. Whilst you are not their teacher or support worker any more you should think very carefully before accepting their request. Young people may have younger siblings or friends still in the school too so we would recommend that you do not accept the request.

! Scenario

You receive a friend request from a colleague who is also the parent of one of the pupils you teach.

What is the school policy?	Always be clear on your school's policy and follow it.
What could go wrong?	Pupils and other parents may be able to see your content through this colleague.
How to decline	This is a socially awkward situation but your colleague should understand this. Reply online and explain your concerns or talk to them. If your school has a clear policy on this then you could make your colleague aware of this.

Further information

Childnet - Teachers and Professionals section	www.childnet.com/teachers-and-professionals
UK Safer Internet Centre- Teachers and school staff section	www.saferinternet.org.uk/advice-centre/teachers-and-school-staff
Social media guides	www.saferinternet.org.uk/safety-tools
Childnet – Using Technology Safely Checklist	www.childnet.com/resources/educators-pack-for-online-safety-awareness
Professionals Online Safety Helpline (POSH)	0844 381 4772 or email: helpline@saferinternet.org.uk
Childnet - How to make a report	www.childnet.com/resources/how-to-make-a-report
UKCCIS Sexting Guidance for Schools and Colleges	www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Childnet International
UK Safer Internet Centre
Co-financed by the Connecting Europe Facility of the European Union