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