Duncombe School

An Independent Preparatory School and Nursery

Duncombe School
Safer Internet – Guidance for Parents

To support our ongoing commitment to Safeguarding and eSafety, our pupils will be doing some age appropriate work in school around safe use of the internet. This Safer Internet Guidance for Parents will back up this work.

What could we be doing?

The following suggestions are part of the advice given to parents and carers by CEOP – the Child Exploitation and Online Protection service.

- **Talk**

Talk to your children about which apps they are using on their devices – ask them what they are for. Perhaps ask them to teach you how to use the technology (children love knowing something we don't). You may need to do this fairly frequently as the landscape changes very quickly and new apps are coming on line all the time. Even if you knew what they were using in the past does not mean they are still using the same software now.

Talk to them about the information in this document – the potential problems and solutions. We do not want to scare our children but knowledge is a powerful tool.

- **Check privacy settings**

Check what **privacy settings** are in place on the all apps/sites. Even apps that do not appear to be social networks provide the opportunity for people to learn about or contact children. Many apps/sites/games have privacy settings which will allow you to choose how visible you are to others. Many default to limited or no privacy so these **settings need to be changed manually**.

For example, the options below are from the video chat application *ooVoo*:

- **Anyone** - your photo, ID & display name will be visible to everyone. Your gender and date of birth can be hidden.
- **People who know my email address or ooVoo ID** - your photo, ID & display name will be visible to people that know you, your name, email or ID. Your gender and date of birth can be hidden.
- **Nobody** - you will be completely unsearchable to everyone. You can invite friends but they cannot invite you

Our recommendation would be for privacy to be set at the highest level – in this case ***Nobody.*** **Many apps/sites default to limited or no privacy so these settings need to be changed manually. When the app updates automatically privacy settings may change without you knowing so it is worth checking regularly.**

Many mobile apps will also default to showing the users location using GPS. You may need to turn this off manually. If these or similar privacy options are not available **please do not allow children to use the app/site.**

- **Share**

Please try and share access to the internet with your children and be involved in their digital lives. You don't have to be sat next to them but being able to walk past on occasion and take a look is a really effective way of ensuring that they use these apps sensibly. Talk to them about what they are posting. If they don't want to talk to you about it then they probably know it is not a good idea.

- **Use parental controls and filters**

Major internet providers and games consoles/device manufacturers allow parents to control childrens' access to the internet. The UK Safer Internet Centre contains useful guidance.

- **Take note of age limits**

Some apps/sites have age limits. They are there for a reason – please do not encourage pupils under these age limits to use the app/site. Allowing children to 'piggy pack' on a parents' social network account is also discouraged as most adults have privacy settings set far lower that one would advise for a child. PEGI ratings are also an effective guide to whether children should be playing a particular game.

- **There is no 'safe' way to be unsafe**

Children and young people sometimes view apps/sites as 'safe'. Snapchat is a good example of this as anything posted on the app disappears after a short time. This makes it *seem* safe and therefore there is no need to be sensible. The problem is that this does not prevent people from taking a screen shot or using other technology to save and keep these images. There is no software that makes it 'safe' for children to share personal information about or inappropriate images of themselves.

- **Follow up**

Many of the pupils will have discussed how to stay safe online. Ask them to tell you. Hopefully they will share some of the following pointers. Pupils in Yr4-6 will be covering these issues after ½ term though they should be able to tell you quite a bit already from previous work.

- Don't interact with people online that you do not know in real life
- Don't trust that people online are who they claim to be
- Don't give out personal information – eg address, telephone number, school

- Don't post anything they would not be happy for a grandparent to see
- Never, ever agree to meet with someone they have met online
- If they are unsure or worried, tell a parent or a teacher

You might want to have a look at this clip as it has been used with many of our Year 5 and 6 pupils in the past. https://www.thinkuknow.co.uk/parents/Primary/Conversation-Starters/Go-to-the-movies/

Younger pupils may have watched CEOP's **Lee and Kim's Adventure**: https://www.thinkuknow.co.uk/parents/Primary/Conversation-Starters/Go-to-the-movies/

How are children and young people using the internet?

These are popular apps and sites that have been used by children in Britain (some more than others of course). It may be a useful guide for you to know what these apps actually do and what the potential dangers are. The list is far from exhaustive and there are many, many other apps/sites available.

All the apps/sites marked with * have a 13 or higher age limit so are not suitable for use by primary age pupils. Some have a check box where new users have to state they are over this age, many do not but it is included in their terms and conditions which new users have to agree to.

Application/website logo as appears on mobile device/desktop	What is it used for?	What are the potential risks to children and young people?
YouTube*	Video Sharing	Access to inappropriate content
PInterest*	Photo/image sharing	Pin boards can be followed allowing potential offenders to learn a child's interests
Whatsapp	Private and group messaging	Messages can be instantly broadcast to large groups
Bitcoin	Virtual currency	Known to be used in criminal transactions
Skype	Video calls	Webcam feeds can be recorded and faked
Facebook*	Social networking	Unwanted contact from strangers
Ask.fm*	Anonymous question based social networking	Cyberbullying
Snapchat*	'Self Destruct' photo messaging app	Photos can be grabbed via screenshot and shared with others

Club Penguin	Massively multiplayer online game	Unwanted contact from strangers posing as children in the virtual world
oovoo*	Video chat	Unwanted contact from strangers
Clash of Clans	Massively multiplayer online game	Unwanted contact from strangers posing as children in the virtual world
Minecraft	Massively multiplayer online game	Unwanted contact from strangers posing as children in the virtual world
Yik Yak*	Anonymous location based 'bulletin board'	Cyberbullying
Facebook Messenger*	Instant messenger for Facebook friends	Unwanted contact from strangers
Blackberry messenger	Instant messenger and video calls	Messages can be broadcast to whole network. Pins are easily shared and accessed
Vine*	6 second video sharing	Exposure to inappropriate content
Moshi Monsters	Virtual game aimed at 6-14 year olds	Unwanted contact from strangers posing as children in the virtual world
Tinder*	Location based dating	GPS reveals child's location
Instagram*	Photo/image sharing	Feeds can be followed allowing potential offenders to learn a child's interests
Facetime	Video chat	Webcam feeds can be recorded and faked
Kik*	Social networking	Exposure to inappropriate content
Twitter*	Social Networking	Trolling abuse
Grindr*	Male to male location based dating	Exposure to inappropriate conversations and images

Whisper*	Anonymous social networking	Cyberbullying
Tumblr*	Social networking and blog host	Exposure to inappropriate material
Skout*	'Flirting' app and social network.	No age verification on users. Geo-location function
Burn Note*	'Self Destruct' messaging app (text only)	Cyberbullying
Omegle*	Online video/text chat between strangers	Frequently used by people seeking sexual chat. Explicit language
MeetMe*	Social Network/chat site	Open network. Geo location function
Tik Tok	Video sharing	A social network for sharing user-generated videos, mostly of people lip-synching to popular songs

Where can I go for help and more information? (click the image to follow the link)

Age appropriate content and also a parent/carer section. Lots of games and activities for children. Set up and run by CEOP.

National Crime Agency's CEOP Command. Click CEOP allows parents and children to report incidents and concerns.

Resources for schools and parents. Lots of really useful practical advice to keep the whole family safe when online. Includes a 'Parents Guide to Technology'.

PEGI ratings are given to games much as certificates are awarded to films. They are a guide to the suitability of the game and also indicate game content through symbols on the game packaging.

If you have any eSafety queries please contact us at office@duncombe-school.co.uk.