



Duncombe
School

An Independent Preparatory
School and Nursery

Duncombe School

Safer Internet – Guidance for Parents

To support our ongoing commitment to Safeguarding and E-Safety, 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 online 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**.

Our recommendation would be for privacy to be set at the highest level. **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 do not have to be sat next to them but being able to walk past on occasion and glance at the screen is an effective way of ensuring that they use these apps sensibly. Talk to them about what they are posting. If they do not 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 children's access to the internet. The [UK Safer Internet Centre](https://www.thinkuknow.co.uk/parents/parents-protecting-their-children-from-online-safety-issues/) 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 'piggyback' on a parent's social network account is also discouraged as most adults have privacy settings set far lower than would be advised for a child. PEGI ratings (<https://pegi.info/what-do-the-labels-mean>) 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 or inappropriate images of themselves.

- **Follow up**

Many of the pupils will have discussed how to stay safe online and will remember their previous learning. Pupils will be covering these issues regularly but there is a particular focus at the beginning of the academic year and during Safer Internet Week in February. Ask your child to tell you about how to stay safe on the internet. Hopefully they will share some of the following pointers.

- Do not interact with people online that you do not know in real life
- Do not trust that people online are who they claim to be
- Do not give out personal information. For example: address, telephone number, school
- Do not post anything they would not be happy for a grandparent to see
- Never agree to meet with someone they have met online
- If they are unsure or worried, tell a parent, teacher or trusted adult

The three-episode '**Play Like Share Band Runner**' resources for 8-10 year olds have been used in the Upper School to highlight the importance of online safety.




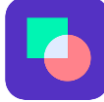




<https://www.thinkuknow.co.uk/parents/playlikeshare/>





Whereas, younger pupils may have watched and explored online safety through the **Jessie & Friends** resources. <https://www.thinkuknow.co.uk/parents/jessie-and-friends>







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 do and what the potential dangers are. The list is far from exhaustive and there are many, many other apps/sites available. The Net Aware website is extremely useful to find further up-to-date information about a specific app. www.net-aware.org.uk

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 must state they are over this age. Many do not but it is included in their terms and conditions which new users must 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 streaming including live streaming	Access to inappropriate content.
 TikTok*	Formerly called Musical.ly. Social media platform that lets you create, share, and discover 60 second videos	Exposure to inappropriate content. Unwanted contact from strangers. Potential offenders can see videos and comment on them. Trolling and cyberbullying.
 Pinterest*	Photo/image sharing	Pin boards can be followed allowing potential offenders to learn a child's interests.
 Byte*	A video sharing app that lets you shoot, upload, and share six second videos	Exposure to inappropriate content.
 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.
 Skype*	Video calls	Webcam feeds can be recorded and faked.
 Facebook*	Social networking	Unwanted contact from strangers.

 Twitter*	Social networking	Trolling abuse and cyberbullying.
 MeetMe*	Social networking/chat site	Open network. Geo location function.
 Ask.fm*	Anonymous question based social networking	Cyberbullying.
 Tumblr*	Social networking and blog host	Exposure to inappropriate material.
 WhatsApp*	Private and group messaging	Messages and phone number can be instantly broadcast to large groups.
 Snapchat*	'Self-destruct' photo messaging app	Photos can be grabbed via screenshot and shared with others.
 Facebook Messenger*	Instant messenger for Facebook friends	Unwanted contact from strangers. Sharing of inappropriate content.
 Kik*	Social networking	Exposure to inappropriate content. 'Meet New People' feature lets you start a conversation with random users.
 Whisper*	Anonymous social networking	Cyberbullying and trolling.
 Club Penguin	Massively multiplayer online game	Unwanted contact from strangers posing as children in the virtual world.
 Clash of Clans*	Massively multiplayer online game	Unwanted contact from strangers posing as children in the virtual world.
 Minecraft	Massive multiplayer online game	Unwanted contact from strangers posing as children in the virtual world.
	Massive multiplayer online game with up to 100 live players	Inappropriate content (heavy violence). Unwanted contact from strangers posing as children in the virtual world.

Fortnite: Battle Royale		
 Roblox	Online gaming site	Cyberbullying and unwanted contact from strangers.
 Friv	Online gaming site	Exposure to some violent content.
 MovieStarPlanet	Online gaming site	Unwanted contact from strangers.
 Tinder*	Location based dating	GPS reveals child's location.
 Grindr*	Male to male location-based dating	Exposure to inappropriate conversations and images.
 Skout*	'Flirting' app and social network.	No age verification on users. Geo-location function.

Where can I go for help and more information? (Right click the images below to follow the links.)



Age appropriate content and has 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 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 indicate game content through symbols on the game packaging.

Net Aware

Bringing together the NSPCC's expertise in protecting children and O2's tech know-how, Net Aware has key information on how to keep your children safe online, including guidance on the most popular apps.

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