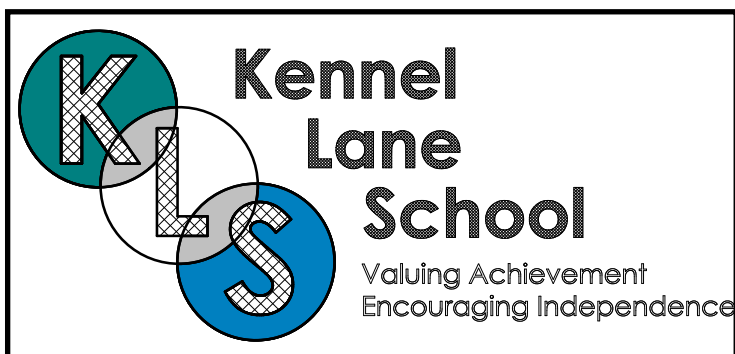


12 Online Safety Tips for Children with New Devices



Christmas has flashed past and we are sure some lucky learners will have excitedly torn the wrapping off a new mobile phone, tablet or games console. For some of them, it will be the first time they've owned a device that connects them to the online world. Even for older learners, a new device means new corners of the digital landscape to explore – and, unfortunately, new risks to be aware of.

We've put together our top tips so that you can guide your young person in enjoying their new digital gifts safely and responsibly. Throughout the year to come. Happy New Year.

1. Always set a password

If your child's new device has a password protection feature, use it! It will help to keep their private information safe and will deny access to their device without permission. Your children's passwords should be something memorable to them – but something which other people can't guess. It's also essential parents write it down in case it gets forgotten!

2. Set up Parental Controls

This really is an essential when you child gets a new device, so they are protected from the outset. It is never too late if you haven't done this already. Most phones, tablets and consoles allow you to customise their settings to determine which games your child can play, how they can communicate (and who with), what content they can access and so on. It will give you peace of mind that they can't inadvertently do something they shouldn't.

3. Pay Attention to Age Ratings

One of the first things children want to do with any new device is play games and explore apps. Before they download anything or install a new console game, check its age rating. Many popular games and apps have content that's not suitable for younger ages. The safest long term solution is to adjust the device's settings so they can only download and use games and apps appropriate for their age.

4. Keep Numbers and Devices Private

Make sure your child understands that they should never share their phone number with someone they don't know or accept a friend request from them. They should also appreciate that it is a good idea to mainly keep their device out of sight, never lend it to a stranger or put it down somewhere where other people could steal it or take it to use without asking.

5. Have the Money Conversation

Before your children start using their new device in earnest, talk to them about in-app purchases and other ways that money might well be spent through their device. Once they understand, you might want to agree on a spending limit and reassure them that they can come to you if they are uncertain, or if they have made a purchase by accident.

6. Discourage Device Dependency

Of course children who have just got a new device will naturally want to spend as much time on it as possible. But whether they are zapping bad guys, watching videos or connecting with friends, it's easy for them to get attached very quickly. Gently remind them that having family time, going outdoors and getting some exercise, are still fun too. The device will still be there when they get back.



7. Explain Secure WIFI networks

Your home WiFi is protected by a password that only your family knows, whereas public networks (like those found in coffee shops, for example) can be accessed by anyone. It is important that your child grasps this difference because; if they're using a device on an unsecured network, then a hacker could access their personal information without them even knowing.

8. Limit Screen Time

Using a device for too long especially just before bedtime, can interfere with a child's sleep quality and reduce their concentration and overall enthusiasm. It might be helpful to agree on certain times of day when they don't use their device. Most devices' settings let you specify a screen-time limit, helping your child stay fresh and focussed in order to perform well at school.

9. Only Pair With Known Bluetooth Devices

Your child may want to connect to another device via Bluetooth, so they can listen to music wirelessly or share pictures and videos with nearby friends. But, if they use Bluetooth to link to a device that they don't know, they are at risk of a stranger being able to see their personal information or having someone transmit a virus onto their device

10. Turn Location Settings Off

It's safest to disable the device's location services (if it is a portable device) so your child doesn't inadvertently make other people aware of where they are. You can usually do this via the device's privacy control settings. Turning location settings off not only means your child's whereabouts can't be tracked by others, it also significantly extends battery life on the device.

11. Stay Aware of the Surroundings

It is quite common to see adults not looking where they're going while engrossed in their phone. Children are even more easily distracted. In some cases, children have been hit by cars or cyclists (adults too!!) because they were staring at their device and lost track of where they were. Remind your child that screens and walking don't mix. If they need to use their device, they should stop in a safe place first.

12. Be There If They Need To Talk

Even when you have made a device as secure as you can, there's still a possibility of your child seeing something that bothers them, or someone they don't know attempting to contact them. If this happens, listen to their concerns, empathise and reassure them. Once they have explained what happened, you can decide if you should take further action like blocking or reporting another user. CEOP is a very good place to start if you are very worried and wish to report something.

If you are unsure and need more advice with using the internet safely or with setting up any devices you could head over to these websites:

www.nationalonlinesafety.com—there is a free app for parents you can download

www.saferinternet.org.uk—tons of great advice and very easy to navigate on the website

www.internetmatters.org/parental-controls/ - advice with setting up loads of different devices

www.ceop.police.uk—to report an incident of online bullying or online sexual abuse

Still stuck and need advice not covered by the above? Give the school a call.