



Online Safety Newsletter: December 2019

Seasonal Netiquette: Screen Time Rules...

School is finishing and the Christmas holidays are starting and that means that your son or daughter suddenly has a mass of free time and many new gifts to play on. For some children this unfortunately means that they can find a computer and stay on it for long periods of time. Often parents relax the 'technology use rules' 'as it's the holidays', children start streaming more TV on Netflix, increase their gaming or simply become more involved with social media. This can then lead to children not wanting to leave the house until they have binged watch an entire series, or they've finished another level, innocently the abyss has swallowed them whole.

The answer is not an out and out ban as these devices do offer entertainment and a way of keeping in touch with friends, but to set reasonable limits that allow for family time, activities and screen time for media and tech that will bring the family together rather than split it apart in endless battles on device use.

Create a Home Family Agreement. There is a template that you can use on the school website produced by the NSPCC here <https://www.archbishoptemple.lancs.sch.uk/parents-carers/online-safety/advice-for-parents> or you could devise your own which creates a weekly plan that includes activities, media and tech time as well as family time. Set reasonable limits for each and agree to it as a family

Want WiFi? To encourage your little ones to earn their WiFi/Internet time, each evening or periodically change the WiFi password then leave a list of chores or responsibilities that need to be fulfilled before the new password is unveiled.

Ban devices at meal times. Whether you sit down at the table or round a camp fire, agree not to use any technology devices at meal times – and yes parents this includes you! This is an ideal opportunity to bond and talk about your days and more than likely learn much more about your children and they you than ever before.

Pay attention to the people you are with. Posting endless images of gifts to Instagram and spending even more time on social media may be very tempting – but guests could get upset if devices are constantly being checked rather than engaging with them. Lead by example to your children and post when you are alone or having quiet time.

Get involved with tech and Media. These days we pretty much document everything! Encourage your children to use their technology to document family Christmas activities and visits with relatives. iMovie and a range of many other movie creating software give an added element of fun other than just taking pictures and it will provide the family with lasting memories caught on camera which you can treasure for many years.

TicTok (Age 13+)

TicTok is an App for creating and sharing short videos of between 3-15 seconds and short looping videos of 3-60 seconds.

Whilst encouraging creativity and expression caution is needed...

13 is the minimum age, but there is no real way of validating an age so really anyone can download it. Some parents have also expressed concern around inappropriate language in the videos. More importantly accounts can be set to public enabling strangers to contact your children.

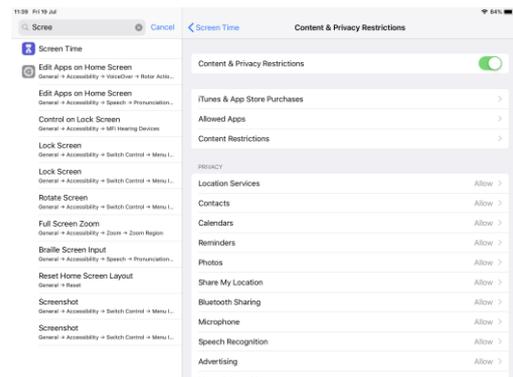
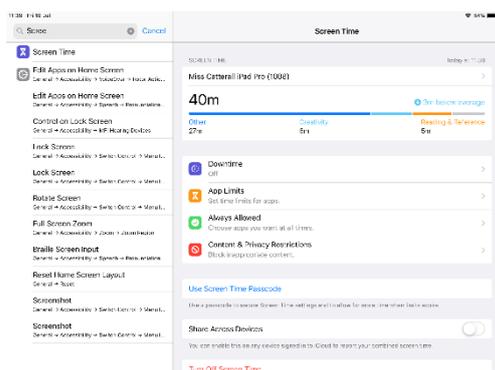
Internet Acronyms

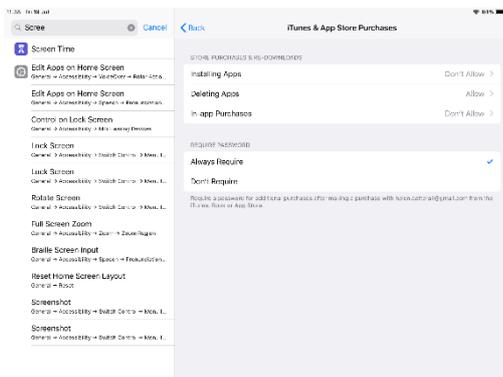
As a result of the recent Online Safety Committee meeting it was suggested that parents may find it useful to have information on all of the different acronyms that are used when direct messaging (DM), here is a list that hopefully will help you to decipher your child's messages.

Acronyms A-L		Acronyms L-Z	
2F4U	Too Fast For You	ITT	In This Thread
4YEO FYEO	For your eyes only	MMW	Mark My Words
AF	As F**k	MOS	Mum Over Shoulder
AFAIK	As Far As I Know	N/A	Not Available
AFK	Away From Keyboard	NaN	Not a Number
AKA	Also Known As	NNTR	No Need To Reply
B2K	Back To Keyboard	noob	Newbie
BRB	Be Right Back	NRN	No Reply Necessary
BTW	By The Way	NOYB	None Of Your Business
CU	See You	OMG	Oh My God
CYS	Check Your Settings	OP	Original Post
DGMW	Don't Get Me Wrong	OT	Off Topic
FYI	For Your Information	PLZ	Please
FWIW	For What It's Worth	SCNR	Sorry Couldn't Resist
FTW	F**k The World	SFLR	Sorry For Late Reply
FML	F**k My Life	STFU	Shut The F**k Up
GR8	Great	TBA	To Be Announced
GTG	Got To Go	TBC	To Be Continued
HF	Have Fun	TBH	To Be Honest
ICYMI	In Case You Missed it	TIA	Thanks In Advance
IDC	I Don't Care	THX	Thanks
IDK	I Don't Know	TTYL	Talk To You Later
IOW	In Other Words	TYT	Take Your Time
IRL	In Real Life	TYVM	Thank You Very Much
KYS	Kill Yourself	WFM	Works For Me
L8R	Later	WTH	What The Hell
LH6	Lets Have Sex	WTF	What The F**k
LMAO	Laughing My Ass Off	YMMD	You Made My Day
LOL	Laughing Out Loud	YOLO	You Only Live Once

In-App purchases

Another topic raised at the Online Safety Committee meeting was the concern from parents about In-App purchasing. This is where additional items such as coins, gems or football players can be bought within Apps such as gaming Apps. If you have this facility enable in the Apple ID it can be a costly affair. A quick and easy way to help avoid any unnecessary purchases would be to use the Screen Time setting available on Apple IOS devices.





To disallow In-App purchases on an Apple device go to Settings>Screen Time and select **Content & Privacy Restrictions**, then select **iTunes & App Store Purchases** and finally **In-app Purchases** you can then select don't allow.

How can I make my home more secure – Advice from CEOP

CEOP is a command of the National Crime Agency that deal with child exploitation

There things you can do to help make your connected home safer for your child:

- 1. Do your research:** Research different products online and read reviews. This is a great way to find out more about a product including age restrictions and credibility, as well as hearing directly from other parents.
- 2. Read the manual:** Read the manual provided by the manufacturers. Information should be given about the privacy of the device, how it connects to the internet, and information about any app which may need to be downloaded in order to use the device.
- 3. Set up parental controls:** Make use of the parental controls available on your home broadband and any internet enabled device in your home. You can find out more about how to use parental controls by visiting your broadband provider's website, or by reading our Thinkuknow article about [parental controls](#).
- 4. Use safe search:** Enable the 'SafeSearch' function on your connected device and web search engines. This will allow you to limit the material your child can see when online. It is important to understand that no parental control or 'SafeSearch' function is 100% effective. This cannot be used alone to protect your child from accessing age-inappropriate material.
- 5. Change the default password:** When you buy a connected device or toy, change the default password. Use a strong password that cannot easily be guessed and do not share this with others.
- 6. Set your Bluetooth to 'undiscoverable':** Many connected devices are Bluetooth enabled. This means they are able to connect to nearby devices without having to connect to the internet. If the device has Bluetooth, set this to 'undiscoverable' so your child doesn't share data or pair with an unknown device.
- 7. Review and/or delete audio files:** Some connected devices or toys work by listening to your child's voice commands, so these devices usually record and keep these audio files to work properly. Refer to the manual and find out how to review and/or delete audio files. If there's a microphone on your child's connected device, you can turn on the 'mute' button. This will stop the device from recording and storing audio files.
- 8. Talk to your child:** Include connected devices in your online safety conversations, reinforcing the message that if your child sees or hears anything that makes them feel worried, they can speak to you or another adult they trust. Read further information on [starting the conversation about online safety](#).
- 9. Supervise your child:** If your child is primary school aged, supervise them when they are online or using a connected device. You should keep the connected devices your child uses in communal areas of the home such as in the kitchen or living room.

Further advice and reading:

https://www.thinkuknow.co.uk/parents/articles/what-is-the-internet-of-things-iot/?utm_source=Thinkuknow&utm_campaign=85b71ed798-TUK GLOBAL DECEMBER 2019&utm_medium=email&utm_term=0_0b54505554-85b71ed798-55025585

https://www.thinkuknow.co.uk/professionals/our-views/how-you-can-keep-young-people-safer-online-over-the-christmas-period/?utm_source=Thinkuknow&utm_campaign=85b71ed798-TUK GLOBAL DECEMBER 2019&utm_medium=email&utm_term=0_0b54505554-85b71ed798-55025585