**A joint presentation by CyberSafeKids and CommSec to River Valley CNS Parents – 4th May 2022**

**DEVELOPING HEALTHY TECH HABITS AT HOME**

This session is aimed at parents of younger children and focuses on establishing and modelling behaviour at home for children who are yet to begin or are starting out on their online journeys. We cover areas such as when and how to introduce technology, managing screen time, sharenting and digital etiquette at home, and offer practical advice and resources to help participants deepen their own knowledge.

Recommended audience: Parents or guardians of younger children.

**PRACTICAL STEPS TOWARD ONLINE SAFETY**

This short session is aimed at parents of younger children and focuses on taking simple no-cost steps to improve the security of your family’s digital environment by protecting your information, devices and online accounts.

[1. Enable parental controls in device settings 2](#_Toc102407429)

[Why? 2](#_Toc102407430)

[How? 2](#_Toc102407431)

[Windows: 2](#_Toc102407432)

[Android: 3](#_Toc102407433)

[iPhone: 3](#_Toc102407434)

[2. Turn off geo-location in 'photos' 3](#_Toc102407435)

[Why? 3](#_Toc102407436)

[How? 3](#_Toc102407437)

[Android: 3](#_Toc102407438)

[iPhone: 3](#_Toc102407439)

[3. Password protect in-app purchases and downloads of new apps 3](#_Toc102407440)

[Why? 3](#_Toc102407441)

[iPhone 3](#_Toc102407442)

[Apple Mac 3](#_Toc102407443)

[Android 4](#_Toc102407444)

[Windows 4](#_Toc102407445)

[4. Enable safe search on whatever search engine you're using 4](#_Toc102407446)

[Why? 4](#_Toc102407447)

[How? 4](#_Toc102407448)

[Google 4](#_Toc102407449)

[Bing 4](#_Toc102407450)

[Duck Duck Go 4](#_Toc102407451)

[5. Consider using 'Google Family Link' (for Android) or Family Sharing (for Apple devices) 4](#_Toc102407452)

[Why? 4](#_Toc102407453)

[How? 5](#_Toc102407454)

[Android 5](#_Toc102407455)

[Apple iPhone 5](#_Toc102407456)

[6. Enable Multi Factor Authentication on your accounts 5](#_Toc102407457)

[Why? 5](#_Toc102407458)

[How? 5](#_Toc102407459)

[Instagram 5](#_Toc102407460)

[Facebook 5](#_Toc102407461)

[Google 5](#_Toc102407462)

[7. HaveIBeenPwned? 5](#_Toc102407463)

[Why? 5](#_Toc102407464)

[How? 5](#_Toc102407465)

[8. Use unique passwords or pass phrases for your accounts 6](#_Toc102407466)

[Why? 6](#_Toc102407467)

[How? 6](#_Toc102407468)

# 1. Enable parental controls in device settings

## Why?

To reduce the risk of your child encountering age-inappropriate content.

With parental controls enabled you can Limit web browsing to appropriate sites and filter mature content from search results. You can also set age restrictions on apps, games, and media downloaded through the Windows and Xbox stores. You can manage screen time, using either scheduling or total time limits. You can also view reports on web browsing and application usage.

## How?

### Windows:

<https://news.microsoft.com/en-in/features/windows-10-parental-controls-feature/#:~:text=To%20turn%20on%20parental%20controls,are%20turned%20on%20by%20default>.

### Android:

<https://support.google.com/googleplay/answer/1075738?hl=en>

### iPhone:

<https://support.apple.com/en-ie/HT201304#:~:text=Follow%20these%20steps%3A-,Go%20to%20Settings%20and%20tap%20Screen%20Time.,Websites%2C%20or%20Allowed%20Websites%20Only>.

# 2. Turn off geo-location in 'photos'

## Why?

By default, many devices record GPS location data within photos taken using the device camera. It is recommended that this feature be disabled so that your child does not inadvertently give away their location if they share photos they have taken, as the GPS information can be easily read by anyone who receives a copy of the photo.

## How?

### Android:

Step 1: Open your phone’s Settings.

Step 2: Open ‘System Apps’ and select ‘Camera’.

Step 3: Disable ‘Save location info’ to hide the location.

### iPhone:

<https://www.lifewire.com/remove-geotags-from-pictures-taken-with-your-iphone-2487322>

# 3. Password protect in-app purchases and downloads of new apps

## Why?

To prevent installation of unwanted apps as well as unwanted expenditure in apps which have already been installed.

### iPhone

Require a password on your iPhone, iPad, or iPod touch

Open the Settings app.

Tap your name.

Tap Media & Purchases.

Tap Password Settings, then choose the setting that you want.

### Apple Mac

On your Mac, choose the Apple menu at the top of your screen, then choose System Preferences.

Click Apple ID.

Click Media & Purchases.

Select the settings that you want for free downloads and purchases. If you have Touch ID turned on for purchases, you won't see this menu.

### Android

Go to play.google.com.

At the top right, click the settings button.

Under "Authentication Preference," select “Require authentication for purchases and app installs”.

Click Update.

### Windows

Password required by default

If it needs to be reset:

Open Microsoft Store and select Profile next to the search box.

Select App settings > Purchase sign-in.

Turn the switch to Off.

# 4. Enable safe search on whatever search engine you're using

## Why?

To reduce the risk of your child encountering age-inappropriate content. Safe search filters out inappropriate results from searches.

## How?

### Google

<https://support.google.com/websearch/answer/510?hl=en&co=GENIE.Platform%3DAndroid>

### Bing

<https://support.microsoft.com/en-us/topic/turn-bing-safesearch-on-or-off-446ebfb8-becf-f035-9eea-b660e8420458>

### Duck Duck Go

<https://help.duckduckgo.com/duckduckgo-help-pages/features/safe-search/>

# 5. Consider using 'Google Family Link' (for Android) or Family Sharing (for Apple devices)

## Why?

Manage time spent on apps and keep track of activity.

## How?

### Android

<https://families.google.com/familylink/>

### Apple iPhone

Set up parental controls with Family Sharing on iPhone

Go to Settings > [your name] > Family Sharing > Screen Time.

Tap the name of a child in your family group, tap Turn On Screen Time, then follow the onscreen instructions.

# 6. Enable Multi Factor Authentication on your accounts

## Why?

To prevent accounts being taken over if username/password is leaked. Loss of access to a child’s account can by itself be disruptive for the child, but additionally may allow an attacker to take on your child’s identity and use that to interact with other children.

Enabling multi factor authentication means that when you try to log in to an account using your username and password you will also be prompted for a one-time code sent to, or generated on, your device. This makes it more difficult for an attacker to take over an account as possession of the device is required in addition to the username and password.

The 2nd factor should be on device under control of parent for additional safety.

Most online services now have the option of enabling multi factor authentication. It is usually quite straightforward to do, as you will see from the examples below.

## How?

### Instagram

<https://help.instagram.com/566810106808145>

### Facebook

<https://www.facebook.com/help/148233965247823>

### Google

<https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform%3DDesktop>

# 7. HaveIBeenPwned?

## Why?

It is a good idea to periodically check your accounts to see if they have been involved in data breaches. We use email addresses to log on to a multitude of services. Those services can be subject of data breach from time to time

## How?

Visit <https://haveibeenpwned.com/> and enter the email address you want to check.

# 8. Use unique passwords or pass phrases for your accounts

## Why?

The danger in password reuse is that if your data is breached on one service that you use, hackers can very easily use widely available tools to automatically check hundreds of other online services to see if that email/password combination works on any of them. They can then take control of those accounts. For this reason it is critical that passwords be unique.

## How?

The easiest way to manage passwords is to utilise dedicated applications such as Keeper, KeePass, or LastPass. These applications store all your passwords in an encrypted database which you protect with a very strong password or pass phrase. From then on you only need to remember that one master password. The password application manages your passwords for you, including generating very strong passwords when registering on websites. Because you no longer need to remember individual passwords you can use passwords like *3Yn@Mp86mPGBGlF$* which are very difficult to break.

<https://www.keepersecurity.com/?data_region=eu> - Commercial

<https://keepass.info/> - Free application

<https://www.lastpass.com/> - Both free and commercial plans