# THE CYBER SAFETY Lady

KEEPING YOU AND YOUR FAMILY SAFE ONLINE



# KEEPING KIDS SAFE ONLINE

## PARENT – TEACHER MANUAL

BY LEONIE SMITH

A step by step guide for safety and privacy settings on social media and computers

# Author Leonie G. Smith



Contact Details

Leonie Smith

Website www.thecybersafetylady.com.au

First Edition May 2011

Latest Revision Sept 2020.

Note: If you see one of these QR codes (image left) through this manual, you can use a QR scanning app on your smart phone to go directly to the link on your phone. Some phones have a scanner built into the camera on the phone. Just open the camera and hold it up to the Code. Or go to your app store to download a QR scanning app to use this link system. The PDF eBook version of this manual has some links included, clicking the urls, will take you directly to the link address on your PC or tablet.

# LEONIE SMITH IS

# The Cyber Safety Lady

Leonie Smith is one of Australia's leading Cyber Safety educators based in Sydney's Northern Beaches in Australia.

She has presented on cyber safety to thousands nation wide. To parents, students, teachers, seniors, corporate groups and industry conferences.

Leonie is the Author of "Keeping Kids Safe Online" an essential cyber safety manual for parents and educators.

Leonie Smith has been endorsed by the eSafety Commissioner as a Trusted eSafety Provider www.esafety.gov.au

Leonie focuses on practical and technical solutions to help every day users of the internet use it safely and in a positive way.

As well as her extensive experience in cyber safety, Leonie was an early adopter of the internet, social media and digital technology.

She has over 20 years experience with internet marketing, online multimedia, managing online communities, and with keeping her own children safe online.

Leonie was a cyber safety ambassador for the 2013 Australian Government's "Stay Smart Online Campaign". She was a founding member and moderator for "Aussie Deaf Kids" an online support group and website for parents of hard of hearing children in 2000.

Leonie's message is overall a positive one about the online world. Her passion is to help all users to enjoy the digital world in a balanced and safe manner.

Leonie Smith is a sought-after media commentator on cyber safety. She has been featured on "60 Minutes", "The Project", "Studio 10", "The Morning Show" and in many other broadcasts and print media.

This manual is a practical step by step guide for online safety for parents and carers concerned about their children's safety and privacy online. Although re-prints are done every few months, there may be some small changes to settings, not yet updated.

# Contents Of Full Copy

# Popular Apps & Social Networks

See more reviews for apps at [www.commonsensemedia.org](http://www.commonsensemedia.org)

**Twitter 13+** Public social media. Live streaming, Has privacy & security settings, blocking. **Dangers:** Bullying in replies, private messaging, re-sharing, extreme adult content, public.

**Facebook 13+** Social Media - Has live streaming, games: privacy settings, blocking. **Dangers:** bullying, privacy issues, fake accounts, adult content, adult contact.

**YouTube 13+ -** Live streaming, has privacy settings & adult content filtering. **Dangers**: bullying, uploading private or embarrassing videos, explicit, extreme content.

**Skype Under 13 with parental consent** voice & chat, share video/pictures/files: privacy settings, blocking. **Dangers**: strangers, bullying, unsupervised messaging, video exposure.

**Tik Tok 13+** Short video recording/sharing, has privacy/parental controls. **Dangers**: Sex/ drugs/alcohol/explicit language - public video, grooming, bullying. Dangerous challenges

**Discord 13+** Online chat site. One to one messaging or private or public group chat. Popular with gamers. Has privacy and security settings to block unwanted friend request. **Dangers:** strangers online, 18+ adult content, predator grooming.

**Snapchat 13+** photo messaging, "disappearing" messages: privacy settings, blocking,. **Dangers**: sexting, adult content, bullying, privacy issues and location map, live streaming.

**Instagram 13+** photo/video sharing: some privacy settings, blocking, live streaming. **Dangers**: Predators, public photos, explicit adult content, fake accounts made to bully, bullying in comments, self-harm, anxiety & depression traps if using for personal validation.

**Houseparty 13+** group video messaging, gaming: **Dangers**: Lack of supervision, strangers being added to groups, or public groups with strangers. Content sharing.

**Minecraft Under 13+ needs parental consent** online game: has single player & private friends-only group play. **Dangers**: swearing, grooming, bullying, some adult content. Minecraft Realms is the safer private subscription version.

# Top Tips For students

## Online Reputation

**Don't:**

- Don't trust others with private video or photos of yourself. Protect your sensitive media.
- Upload or share pictures/videos of others online without permission.
- Take or share nude images or video. Sharing without consent is illegal.

**Do:**

- Be careful what you say and put on the internet. Would mum & dad approve? Can't be undone. Can be copied passed around and downloaded.
- Respect your friend's and your family's privacy, as well as your own.
- Always ask permission before taking pictures/video, or using webcam of other people.

## Privacy

**Don't:**

- Give out your real name or other private details on games and apps. Use a made up name.
- Post home address, phone numbers, school name, passwords, bank details, drivers licence, identity cards, real friends or families names.
- Expose another person's real identity or personal details online.
- Overshare - your privacy is important. Delete or archive old posts.

**Do:**

- Use a "handle" or pseudonym (made up name) for games and apps.
- Set good, secure, passwords & privacy settings on every app/platform/account.
- Log out of accounts and computer when leaving your device or computer.

## Behaviour

**Don't:**

- Participate in "online drama" or bad behaviour. Mute or block.
- "Flag" or report a user to an online moderator out of spite. Get help if frustrated.
- Be a "Troll" (to type something annoying just to get a reaction).
- Be a "Spammer" (send constant messages over and over).
- Be a hacker or an extortionist. Hacking & blackmail is against the law.

# Monitoring Computers

## Placement

- Keep kid's PCs and mobile devices in family rooms. Discourage use in child's bedroom.
- Make agreements for safe internet device use with your children. (Age dependent)
- Buy desktop PCs rather than laptops to discourage mobility. Use a laptop cable lock on laptops if you want to prevent them being moved to a private room.

## Screen Time Limits

- Set time limits on computer - mobile device use. Stick with them as much as practical.
- Ask kids to help set time limits. If they go over time, deduct time for the next session.
- Put device timetable on a notice board or on fridge to prevent disputes. E.g end of manual.
- Include T.V & online social time, messaging, social media, gaming according to age.
- Limit gaming on computers and devices during school week with timetable, digital reminders.
- Give rewards for times adhered to, e.g., gift cards or a special outing, brainstorm ideas.
- Avoid excessively harsh punishments. Fear of consequences may make a child clam up.
- Balance gaming/social media with creative and educational activities on computers. Join in!

## Monitoring

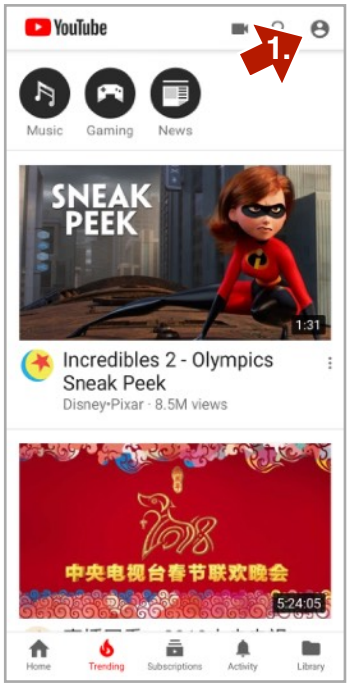
- Check your child's browser history if concerned. Be concerned if child has deleted history.
- Keep control of your child's passwords when age appropriate.
- Use family shared accounts or built in operating software for monitoring - parental controls.
- Monitoring software is great for families with younger children.
- Get involved in your child's computer time. Ask questions. Have fun with them and keep dialogue open. Don't disparage their interest. Share fun videos and games.
- Download and sign up for the same apps as your child uses, and "friend/follow" your child, at a distance, older teens will need privacy and may ask you to un-friend…this is normal.
- Find the blocking and reporting tools, and for younger children find out if the platform has parental controls or adult supervision/moderating that is reliable.
- Find game reviews and ask opinions. Are they too violent or sexual in nature?
- For reliability stick with age classification recommendations on games and apps.

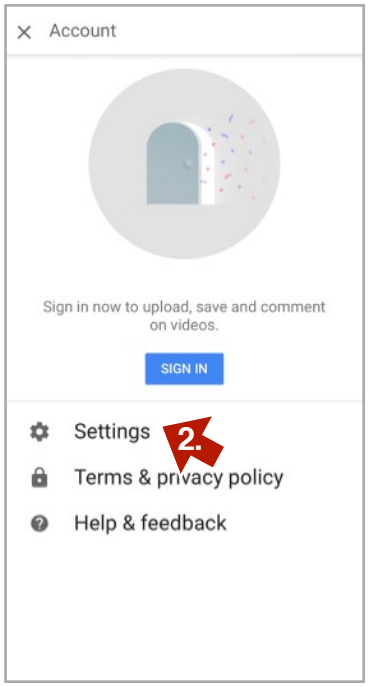
# YouTube Safe Search Apple Mobile App

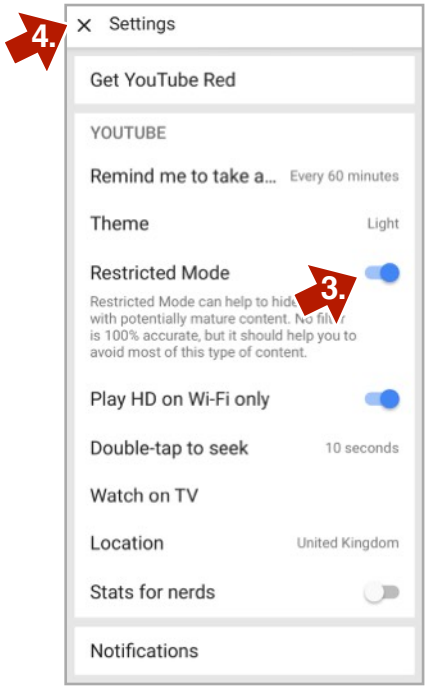
Open YouTube Mobile app - 1. Click profile, top right. 2. Go to Settings menu. 3. Click “Restricted Mode Filtering” to the on position. 4. Click X to exit.

**Android:** Open YouTube app - go to ☰ or(3 vertical dots) “Settings” - “General” - Turn “Restricted mode” on or off.

**Note:** Don’t have to be signed in. Cannot be locked on, a child can change this filter, if they go to settings.

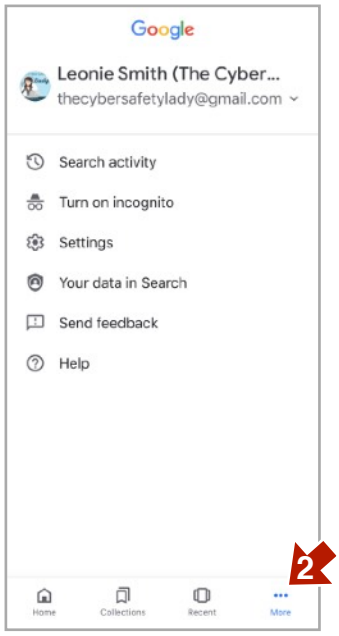


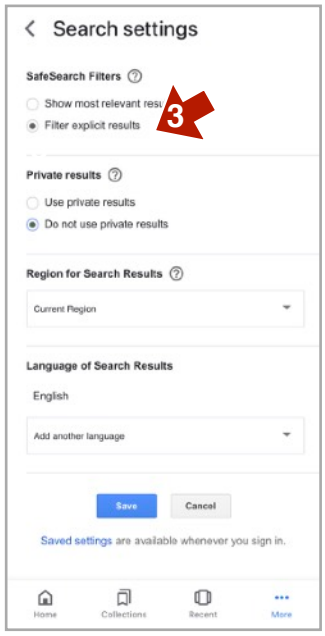




# Google Safe Search Apple Mobile App

1. Open app - 1.Go to profile log in. 2. Bottom right - click … More” 3. Click “General” then “Search Settings” Click “Filter explicit results”, Click “Save”. Click Arrow back to exit out. Set Safe Search on all Browsers and Google apps. For PC settings see **Note: Cannot be locked on with a password**

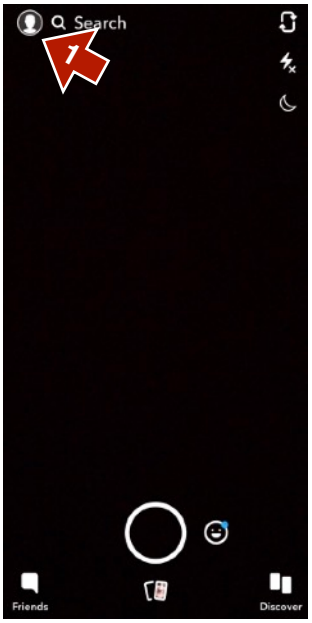



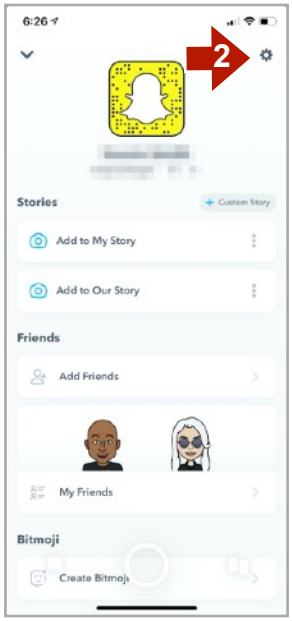

**Android:** Open Google Mobile app. ☰ “Settings” - “Privacy & Accounts”. Scroll down to “Safe Search Filter” and enable.

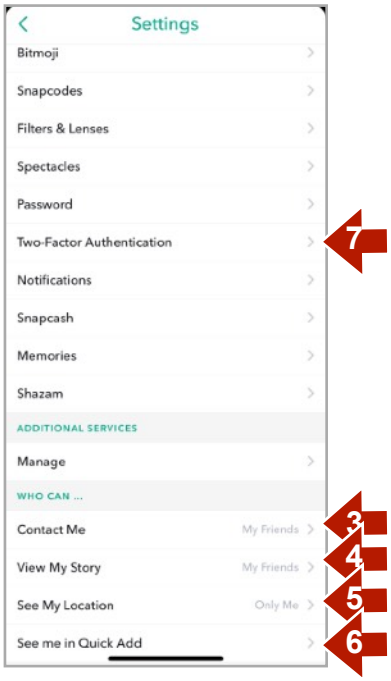
# Snapchat Privacy Settings

Snapchat is advertised as a messaging app where messages “disappear”. However Snapchat photos CAN be screen-shot, saved & shared. Using the “SnapMap” can be risky for your privacy & safety. Enable Ghost Mode via settings & “See My Location” Set to “Only Me”

Settings: Open app - 1.Click profile icon - 2.“Settings” - Scroll to down to “Who Can…” Set 3&4 to “My Friends” Set 5. to “Only Me” or Ghost Mode. 6.Turn off “Quick Add”. 7. Set up TwoFactor Verification, to secure your account from hackers via phone number or an Authentication app like Google Authentication or Sophos Authentication.

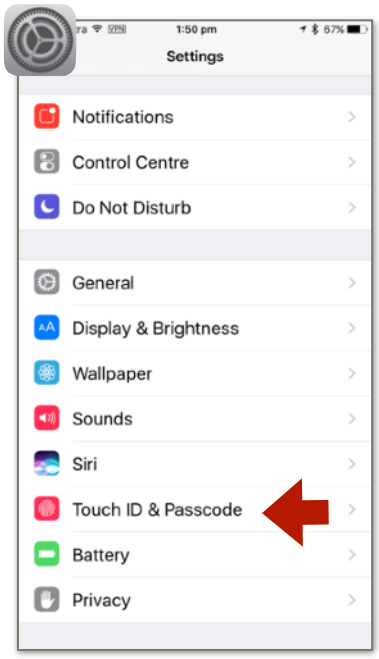


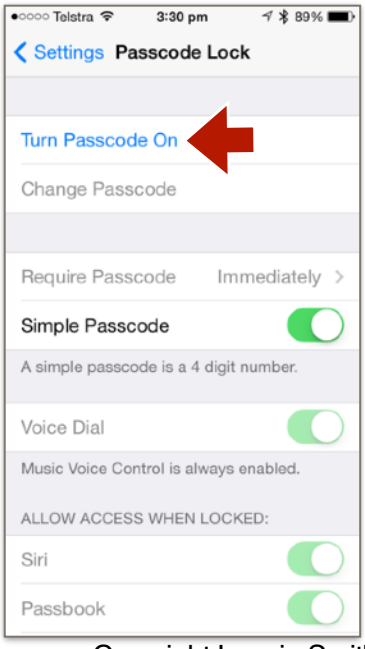



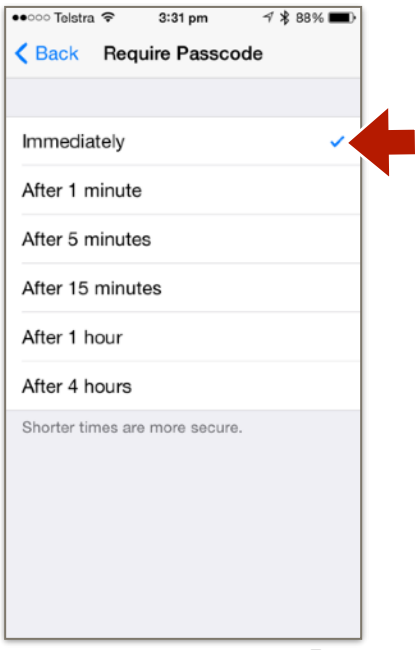




# Setup Screen Lock On Apple Mobile

Set up a secret screen lock passcode, Touch I.D Or Facial recognition. You can set it so that it locks immediately or after a few minutes of inactivity. Go to your device “Settings” - “Passcode” - “Turn Passcode On” - “Set up a pass code” - set the time delay - then exit out to save. Set Touch ID to most secure settings. Select what you have access to when the phone is locked. iPhone X and newer iPhones have Face ID & Passcode settings.



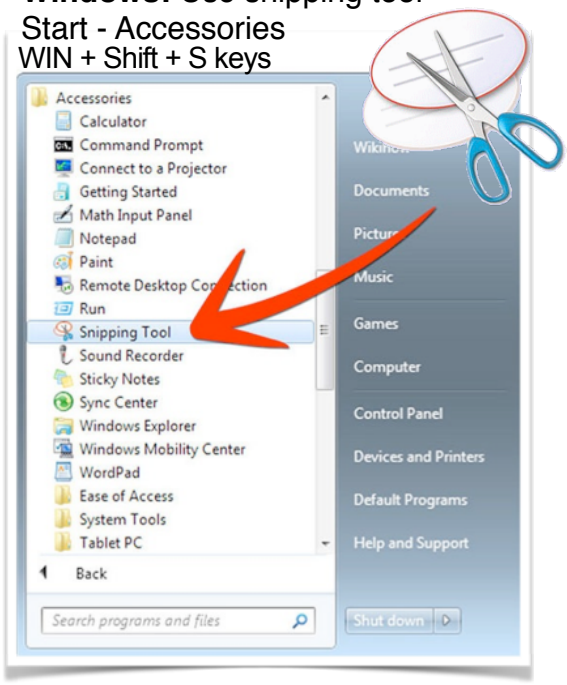



# How To Screen Capture

Screen capture is a good way to keep evidence if you are abused in some way online. If someone has sent you a nasty SMS message don't delete it, save it for evidence. For comments or fake accounts (set up to bully), taking a screen capture of the incident might be the only evidence you can save to take to your school or the authorities to have some action taken, before the user that posted it deletes it.

Alt-Windows Key-Print Screen

**Windows:** Use snipping tool
Start - Accessories
WIN + Shift + S keys




**Mobile Devices:** Press Home and On/Off Switch at same time. iPhone X On/Off and volume up button. Do a search online on how to screen capture, if your device is different.

**Apple Macintosh:** Click Command/Shift/3 (or 4 to capture partial screen.) Be sure to hold down all 3 keys one after the other.


# Parents Guide To Fortnite: Battle Royale 12+

**What is Fortnite: Battle Royale?**

It is a free online multi player survival game, with over 250 million global players and still growing. It is a “last person standing” style battle on an ever shrinking Island, where you play against other online players. This version of Fortnite is incredibly popular in primary schools and junior years of high schools, but also popular with adults. It is fast paced, and drives the player on to gain more skills to last longer in the game, win the battle or take up challenges and gain in game points and rewards. Although you can download the free version and earn in game rewards through play, you can pay for upgrades with currency called V-Bucks for better looking avatars (skins) and tools. There is also a subscription version “Battle Pass” which gives players more levelling up and gear.

**Violence And Guns**

The bright colours, pretty landscapes and creative outfits give this game a sort of “Alice In Wonderland” feel... But there is no getting around the fact that the “Royal” version of the game is focused on killing your opponents with weapons, and defending yourself. Unlike other shooter games, there is minimal gore and blood, there's no blood splatter or horror as such. But as a parent, you would have to be happy with your child playing a game that glorifies guns, weapons, and blowing stuff up. Fortnite is rated 12+ due to the level of violence, exposure to weaponry, and risks in involved if playing with strangers. This game can be quite scary for younger players and distressing if they cannot cope with the gun violence, being killed and hunted. Also there may be high level of frustration due to some very professional players, winning is very hard.

**The Basics:**

- Rated 12+ via the European Pegi standard and T for Teen only for U.S and Canada. Commonsense media suggest 13+
- It is a strategic shooting, last person standing survival style game, with some Minecraft style building and mining, to build fortresses and launch pads.
- There can be up to 100 players in any battle at the same time.
- It is an online multi player game available on PlayStation 4, Xbox One, Windows, and Mac and now mobile devices
- You can connect and play with real life friends who also have the game, link the account to Facebook to find friends, or make friends and play with strangers in the game
- You can play by yourself in Solo Mode, be part of a Duo or part of a Squad with people you know in real life, or random strangers. Creative mode is for exploring and building without the battle, play only with friends or solo.
- The game has voice chat on headset/mic which can be turned off in the settings if you don't want to talk or hear others in your team. You can't hear other players talking other than those on your team.

# Where Are Kids Going Online?

**Supervise Without Spying!**

One of the most important things when raising digital natives is to have a relationship that fosters open discussion about issues that are impacting your child. A relationship that is open and honest is essential when children maybe confused by something online or concerned with making a good decision, particularly around cyber bullying. It is vital that children need to be able to go to their parents or carers to discuss their online concerns without fear.

A child may feel that this is very difficult to do if they believe their parent is not interested, disparaging, or tends to threaten extreme consequences if something goes wrong online. Sharing concerns can also be very difficult if the child feels that the parent has no understanding about digital technology, they may feel that to be able to discuss this issue with the parent, they would have teach their parent before the parent can help.

According to a recent Mcafee survey, 70% of teens are hiding things from parents online. That statistic is quite concerning, even if some readers think it is "normal" for kids to hide things from parents. Secret online interaction is an area just ripe for vulnerable kids to be taken advantage of. I don't agree that this survey reflects normal behaviour by teens and therefor we should not be surprised or alarmed. This figure, indicates the majority of parents have significant relationship and trust issues with their children that they need to work on with or without help in order to adequately supervise their children's online lives.

It is important that parents know where their children are going online to be able to have conversations and open discussions about their experiences, just as it is to know where they are traveling to offline. If you set parental controls, being open and honest about monitoring your child's internet use is essential. "Spying" on your children's online world erodes trust ,and then makes it difficult to talk about things you have found.

In order to have those important conversations about digital device use, it helps to find something that your children are doing that you CAN connect with. It might be that you play a digital game with them, or find other things you can share together on their device that you both enjoy. Perhaps it is sharing video's, memes, puzzle apps, creative software, music.

As the parent YOU need to open up the conversation and keep it going, cyber safety is not a one time only discussion, cyber safety awareness requires constant re-education and sharing of information amongst parents, teachers and children.

# Leonie Smith "The Cyber Safety Lady" Can Help!

Leonie Smith is one of Australia's leading cyber safety experts, she has helped thousands of students, parents, teachers, seniors, childcare workers business and other community organisations to learn how to navigate the internet with better safety.

Leonie is also a cyber savvy mum, she knows what it's like to be a parent with kids who are computer experts. She also knows how hard it is to be a digital parent…yes even for a cyber safety expert!

Though based in Sydney The Cyber Safety Lady travels all over Australia. Take advantage of Leonie's expert advice and set up good habits, privacy settings and internet security now, BEFORE you or your family have a distressing experience online.

## Virtual Presentations

Leonie is now presenting her talks virtually.
See more about her presentations here: https://thecybersafetylady.com.au

### Personal Consultations On Cyber Safety

Leonie also provides parents with personal consultations to help parents set up safer environments on digital tech. https://thecybersafetylady.com.au/services-4/

- Parental Controls
- Screentime timetables
- Information about gaming and apps
- Supervising children online

Leonie Smith is a certified cyber safety education provider with the Australian Government Office of the eSafety Commissioner www.esafety.org.au.

**From A Grateful Parent!**

*"Hi Leonie, without your expertise in all of this I think I would have had my 11yr old son off to the psychologist & completely stressed out myself. You have paved a safe way forward for us, & I feel a lot more in control of what my son is exposed to online"* Many thanks A. Finnegan

To keep up with the latest on cyber safety and privacy you can connect with Leonie on -

info@thecybersafetylady.com.au
www.twitter.com/LeonieGSmith
www.facebook.com/thecybersafetylady
www.thecybersafetylady.com.au
See www.youtube.com/LeonieGSmith
"Digital Families Podcast" https://anchor.fm/leonie-smith0

“Keeping Kids Safe Online" is an up-to-date manual that gives Parents practical advice on how set up social media apps and online platforms safely

This manual is essential for all parents who want to their children to use the internet safely and with privacy.

It includes advice for cyber bullying, privacy settings for popular social media platforms, safe apps, screen time limits.

Keeping you and your family safe online.

Author Leonie Smith
www.thecybersafetylady.com.au