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

www.thecybersafetylady.com.au

Author Leonie G. Smith

Products and company names mentioned hereon may be the trademarks of their respective owners and organisations.

This book expresses the views and opinions of the author. The author will not be held responsible or liable for any damages caused or alleged to be caused either directly or indirectly by this book. The content within the book is provided without warranties. The views and opinions expressed in this book by the author are in no way representative of the author's current or previous employers.

Contact Details

Leonie Smith

Website www.thecybersafetylady.com.au

First Edition May 2011

Latest Revision Oct 2018.

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 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.

She is certified as a qualified online safety educator by the Australian Government Office of the eSafety Commissioner www.esafety.gov.au

Leonie focuses on practical and technical solutions to help every day users of the internet use the internet and social media 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, started 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.

Leonie Smith is a Family Zone Cyber Safety Partner. www.familyzone.com

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 changes to settings not yet updated.

Contents

Popular Apps
& Social Networks

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, privacy settings, adult content filtering.
Dangers: bullying, uploading private or embarrassing videos, very adult content.

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

musical.ly - Tik Tok 13+ Karaoke style singing video recording/sharing, privacy settings.
Dangers: Explicit lyrics, public broadcasting, grooming, bullying, explicit adult content.

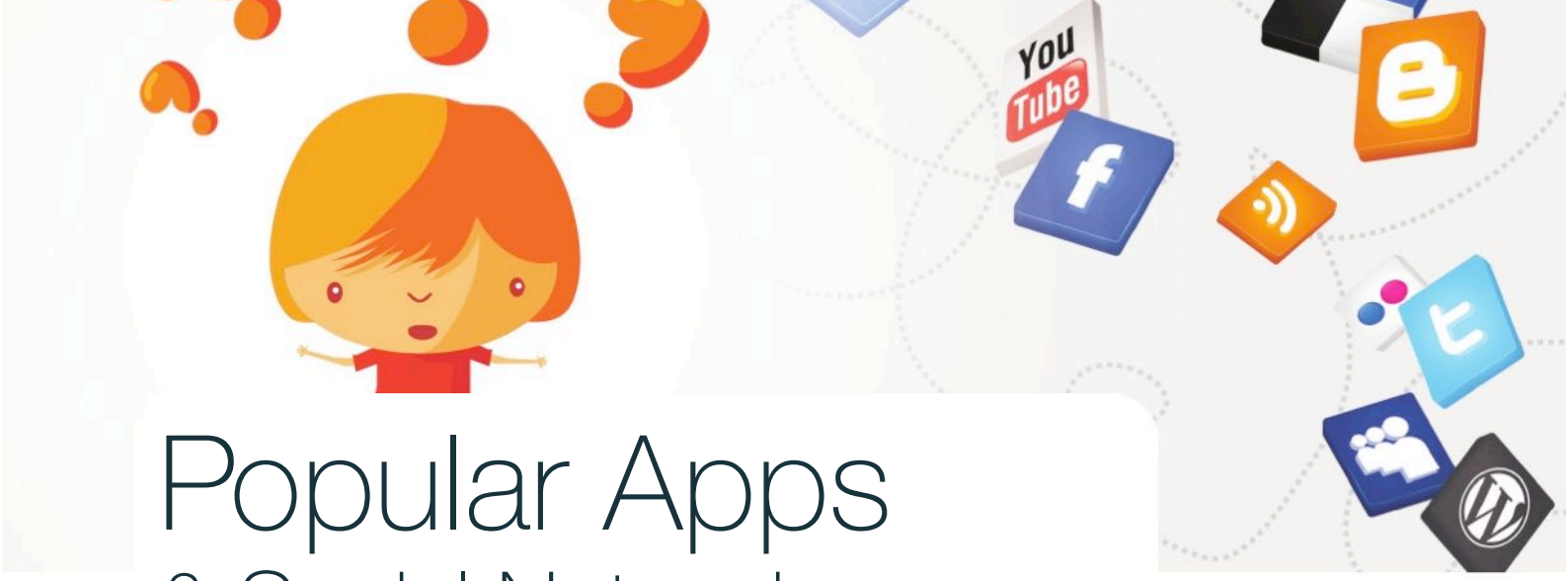
LiveMe 13+ Under 18 with parents permission. Public live video broadcast.
Dangers: Privacy, exposure, Adult followers, cyber bullying via chat, live online grooming, some adults only content.

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: adult followers, public photos, explicit adult content, fake accounts made to bully, bullying in comments, anxiety & depression traps if using for personal validation.

Clash Of Clans 13+ online game: some moderation. **Dangers**: very expensive add-on purchases, swearing, addictive, playing with strangers, difficult to block/ban, grooming.

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.



Popular Apps
& Social Networks

Fortnite: Battle Royale 15+ in Aus Online Multiplayer - Last person standing shooter
Dangers: Strangers - Bad language, bullying - Gun violence - No gore/blood splatter.

Pokemon Go 13+ Online Hunt Game- Outdoor activity: some privacy settings.
Dangers: Location tracking. Dangerous real life locations. Fake copies of the game

Omegle 13+ with parental consent live video chat with random strangers.
Dangers: meeting strangers online, live sexual videos, grooming.

Kik 13+ with parental consent messaging & other apps: blocking. **Dangers**: contains adult apps & content, stranger contact/blackmail, insecure privacy settings, grooming.

Apple Messages 13+ no age limit under parent's family account: secure privacy, blocking **Dangers**: unsupervised messages, stranger contact if email or ph # shared.

WhatsApp 13+ voice/chat messaging - ph # required: no privacy settings, blocking.
Dangers: unsupervised messages, profile sharing on social media encouraged.

Facebook Messenger 13+ voice/chat messaging: privacy settings. Secret Messages.
Dangers: unsupervised hidden messages, linked to Facebook profile. Add on apps.

Tinder 18+ dating "Hookup" app. **Dangers**: meeting strangers, search by location, links to Facebook and Instagram.

Sarahah 17+ Feedback app: blocking. **Dangers**: Known for bullying. Links to Snapchat, Instagram. (Website only, app was removed from app stores Feb 16th 2018)

Roblox 13+ Under 13 with privacy mode/parental controls. Online multi player game. **Dangers:** Stranger friend requests, adult content, bullying, swearing, grooming.

Tumblr 13+ blogging platform: has privacy settings. **Dangers**: "follows" & contact from strangers, explicit adult content, self-harm glorification.

Other Platforms

Browsers: Microsoft Edge, Safari, Firefox, Google Chrome. Danger of accessing adult sites, downloading viruses and spam, safe search filters and parental controls available.

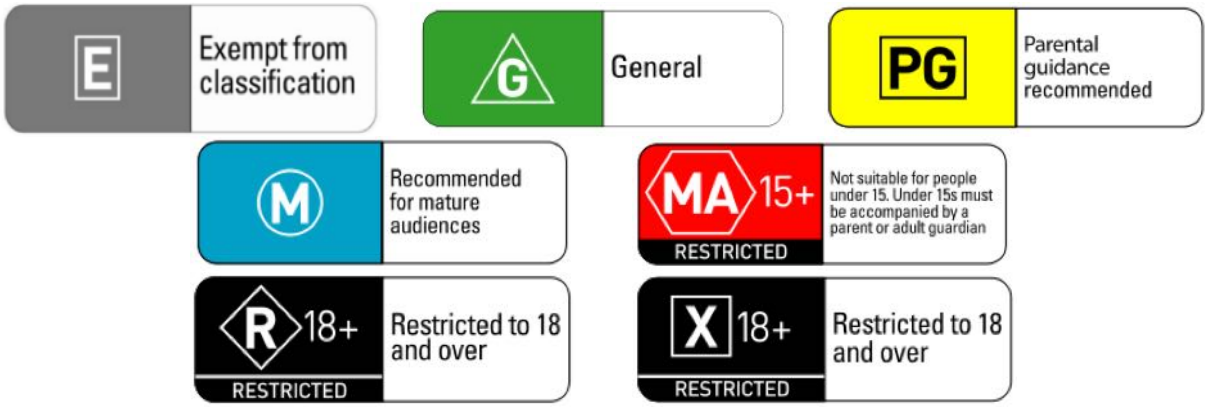
Search Engines: Google, Bing , Duck Duck Go. Danger of accessing adult sites, use safe search filters. (Instructions in this manual).

Email: possible viruses through attachments, “Phishing” (fake email) scams, bullying. Filters and blocking are available on both Apple Mail and Outlook, also through parental controls on Mac and Windows. Use anti virus software.

Texting: danger of over-exposure through photo/video sharing and texting, phone numbers and texts not always easily blocked. iPhone iOS and Android have message & call blocking. SMS & Call Scams.

Classifications

iTunes and Google Play Store age ratings are set primarily by the developers of the apps. Many apps set at 13+ are rated 12+ on the App Stores. They are not a reliable method to use to gauge the suitability of apps. However, if an app is rated 17+ it means that the app contains adult content and is definitely not suitable for minors.



Illegal for under 18 to buy, rent, view.

Pornographic: Under 18yrs to buy, rent, view is considered a Criminal offence.

Top Tips For students

Online Reputation

Don't:

- Don't trust others with private video or photos of yourself. Protect sensitive media.
- Upload or share pictures/videos of others online without permission.
- Take or share nude images or video. It is illegal under age 18, you could be charged.

Do:

- Be careful what you say and put on the internet. Would mum & dad approve? Can't be undone. Can be passed around, copied 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.

Bullying

Don't:

- BE a bully, you may be reported and lose your account. You can be arrested and charged with harassment or cyber bullying if you join in or abuse others on the internet.
- Stand by if you see or hear bullying. Report to a responsible adult. You can help.
- Respond to bullies or "Trolls" by arguing or defending. Block, Report, Support.
- "Re-friend" a bully unless you are sure you are safe. Ask parent if not sure.

Do:

- Support the victim and tell a responsible adult.
- Save copies - Screenshot. Mac-Cmd/Shift/4, Win-Print Screen or snipping tool.
- Block the bully & tell your parents or a responsible adult straight away. Do the same if you feel uncomfortable about a message.
- Be a good friend online. You can make a big difference by being an upstander to bullying.

Safety

Don't:

- "Friend/follow" random strangers. They might be an adult NOT a child. Not all children are safe to "friend" either. This includes online games like Minecraft, Roblox, Fortnite.
- Agree to meet an "online friend" in real life, unless accompanied by a trusted adult.

Do:

- Alert parents or teacher if an adult stranger starts chatting to you online. Block the stranger.
- Tell your parents if you are sent something upsetting or rude online. They need to know.
- Do play safe, age appropriate games, and use age appropriate apps. Check age ratings.

Viruses And Malware

Don't:

- Click pop-ups on browsers, it might be spam or a virus. Click X or escape.
- Open attachments or click links in emails if you are not expecting them.
- Click links on social media if you don't know where they are going.
- Download things from the internet without checking with a parent. Beware of fake apps and "Find More Friends" style apps. Be careful of game mods and weird program updates.
- Leave your privacy settings set to public. Do protect your privacy.
- Download stolen games or films. It's a crime. You may be caught. Some contain viruses.
- Answer phone calls or messages from people you don't know. Block them. Don't call back.

Do:

- Only download apps/games from reputable stores like iTunes, Steam or Google Play.
- Tell parents if you see an alert about a virus. Be careful though, it might also be a scam.
- Set strong passwords, 8 characters, upper & lower case letters, include numerals.

Monitoring Computers

Placement

- Keep kid's PCs and mobile devices in family rooms. Discourage use in child's bedroom.
- Make agreements for mobile device use in bedrooms and time limits for older teens.
- 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 digital 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 computer timetable on a notice board or on fridge to prevent disputes.
- Allow online social time including texting, Facebook, Skype, gaming limit 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.
- 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 like "Family Zone" 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.

Get Involved!

- Find out what online words and acronyms mean and have fun with that. LOL, YOLO etc.
- Ask kids to teach YOU about what they know - guide you through a game.
- Teach children how to block and report on every online program they use.
- Talk to kids about online privacy, bullying and predatory behaviour BEFORE issues arise.
- Find family games and apps to share - suggestions in this manual.
- Find creative, exploratory and educational games also on my website:
- http://thecybersafetylady.com.au/category/family-game-reviews/ and www.commonsensemedia.org.
- Set boundaries around online behaviour inside and outside your home. Be clear about your expectations of what games and apps they are allowed to use.
- Give your children ideas for how they might avoid playing games or using apps they are not allowed to use if pressured by friends. Reward them for compliance.

Supervision Has Its Limits

Note: Supervising and "friending" your child on apps and social media is no guarantee of their ongoing safety. Your child's content can be shared beyond their friends' lists. Nasty comments can be added to your child's post to upset your child and then shared publicly or privately, regardless of your supervision.

Your child is only as safe online as their friends allow them to be. If your child's friends don't have adequate adult supervision, are immature and unkind, then your child is at risk.

Children who use apps designed for an older age group may not be mature enough to handle the environment that they are signing up for, despite your supervision. Only allowing age appropriate apps and games is vital for a safer online experience. Delay social media use.

Although the iTunes and Google app store age restrictions are often not very accurate, if an app is listed as being for 17+ or R18+ there is usually a very good reason for this. Find out why! Search online for the name of the game or app your child wishes to use to see what other parents and reviewers say about it.

Or search for the app/game on either of these websites-

The Cyber Safety Lady
http://www.thecybersafetylady.com.au

Common Sense Media
http://www.commonsensemedia.org

Report cyber bullying & image based abuse to the platform/app concerned see this list of reporting links for the most common apps and social media from "Cyber Bullying US".http://cyberbullying.org/report/ Report bullying, image based abuse, stalking to https://esafety.gov.au (Aus only)

Report cyber crime to your local police, and fill out the step-by-step form at - Australian Cybercrime Online Reporting Network http://acorn.gov.au
Scams to www.scamwatch.gov.au

Online Security

- Set different passwords for every account. Use eight digits or more, mix upper and lower case, numerals and symbols. For example - Fine*9SillyPaper - Don't use any related words.
- Set a screen/login password on all computer/mobile devices to prevent unauthorised use.
- Password manager software is a good option for users with a lot of passwords.
- Make sure all antivirus software is up to date and still valid. Set to update automatically.
- Software updates often help to block new viruses and malware, update regularly.
- Check firewalls are switched to "On" on routers and computers through security settings.
- Set unique passwords on all internet connected devices, including baby monitors and internet connected speaker assistants like Apple Pod, Amazon Alexa & Google Home.
- Some free public Wi Fi access is insecure. Use only reputable Wi Fi sources.
- Use Paypal, pre-paid credit cards or software gift cards (available from gaming/electronic stores and supermarkets) rather than credit cards when paying online.
- Set up two-factor verification apps & secret pins or passwords on your accounts to prevent your accounts being hacked. When logging in from a different browser or devices you will then receive an SMS or app notification on your mobile device to verify your account.

  Facebook - Go to - Account - Settings - Security & Login - 2 Factor Authentication

  Apple - https://appleid.apple.com - Manage ID

  Google - www.google.com.au/landing/2step

  Twitter - https://twitter.com/settings/security security and privacy

  Microsoft/Skype - https://account.live.com/proofs/Manage
- Set security and privacy for Google accounts here: https://myaccount.google.com
- Don't open email attachments or click links in emails unless expecting them. Don't click links in emails where you are asked to "Update your account details" Always go to your account via the official website address, or ring your provider using usual phone number .
- Watch out for Fake emails, and SMS & phone calls from claiming to come from reputable institutions. Go to the website via search or the web address rather than click a link from an email, SMS or Message to update account details. Don't ring number back on messages.
- Report Cybercrime ie scams, identity theft, hacking to acorn.gov.au & scamwatch.gov.au. Cyber Bullying, stalking & Image based abuse eSafety.gov.au and your local police.

Phone Privacy & Safety

Do:

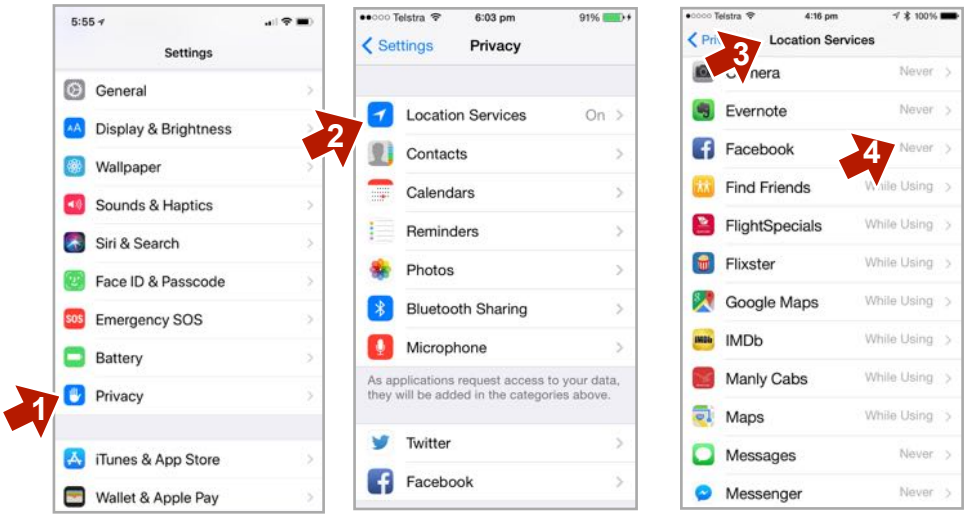
- Set screen passcode, fingerprint or face I.D to prevent unauthorised use.
- Set up “Find My Phone” on iPhone settings. Android also now has Find My Phone & there are several “Find My Phone” apps on Google Play, or use Android Device Manager App.
- For Android security settings navigate to “Settings” - “More” - “Security” and enable “Verify Apps” Un-tick “Unknown sources” Or “Settings” “Personal” “Security” “Device Admin” Tap “Unknown Sources”
- Use message/call blocking for scams or bullies. (Instructions in this manual)
- Share your mobile number only with close friends or family. Avoid putting online.
- Protect your location. Turn off location services on apps that don’t require it (see below).
- Report anything upsetting you are sent on your phone. Students should tell a trusted adult.

Don’t:

- Give your phone to another person to use, unless very trustworthy.
- Download dodgy apps from obscure app stores or websites. Check ratings first.
- Use your phone for spammy texting or bullying.
- Take photos/video/recordings without permission, or of embarrassing or bad behaviour.
- Share photos/videos without permission of all the people in the photo/video.
- Take a nude selfie or you might regret being posted around. Phones can get hacked.

Note: Taking or sharing nude photos of people under 18 years of age is illegal.

To Disable Location Services On Apple Mobile



On **Android** devices, tap the “Location” option from the “Settings” menu.

Step By Step Safety & Privacy Settings

YouTube Kids App 4+

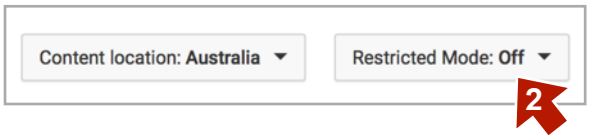
There is now a kids version of YouTube, available on iTunes and Google Play for children under 13 years. It contains advertising, and primarily relies on an automatic filter to curate the videos. There are parental controls where you can select the videos your child watches, but parental supervision is essential. There have been recent reports of inappropriate videos on YouTube Kids. See Page 19 for details.

YouTube Safety - PC - Laptop settings

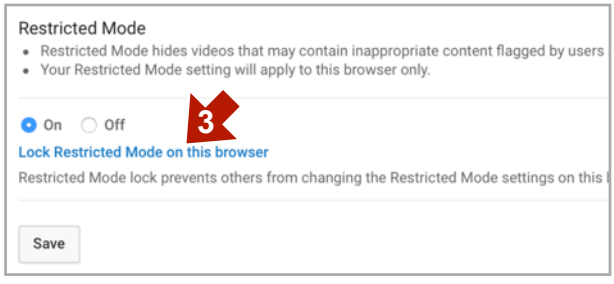
To prevent most adult content on YouTube, “Restricted Mode” settings must be put on every browser profile and YouTube app on every computer and mobile device your child uses. All browsers such as Google Chrome, Safari, Microsoft Edge, Mozilla, Firefox and Opera, if used, must be set. It’s not a difficult process, but easier with less browsers installed. Note: This setting is not Cloud based has to be set on all browser profiles on all devices.

1. For P.C YouTube go to http://www.youtube.com and if you have an account, sign in. If you do not have an account create one.

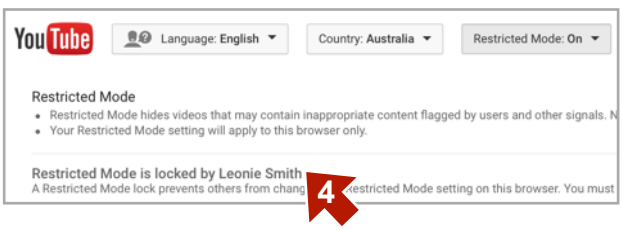
2. When signed into your account, click your profile pic, top right then Click “Settings” (don’t click “Restricted Mode from the dropdown menu, It doesn’t lock this setting on) & scroll to the bottom of the YouTube page to find the “Restricted Mode” in bottom menu tab. Click to set it from “Off” to “On”.



3. Also click “Lock Restricted mode on…” re-enter your YouTube password, then click “Save”. This is to prevent your child turning it off on this browser.



4. Sign out of your account. Only you can change the safety settings now. Reverse procedure to unlock. **Note:** Make sure your password is not saved on your browser so that your child cannot log in to YouTube using your account.

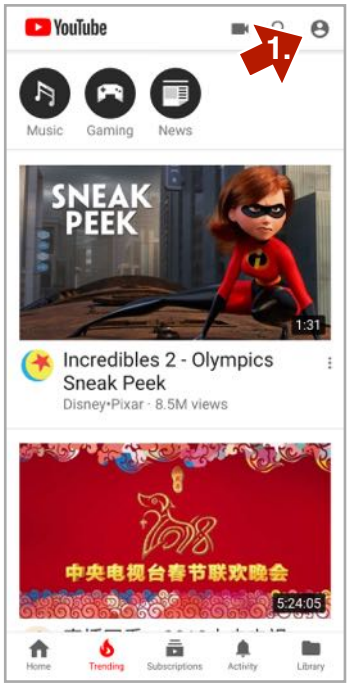


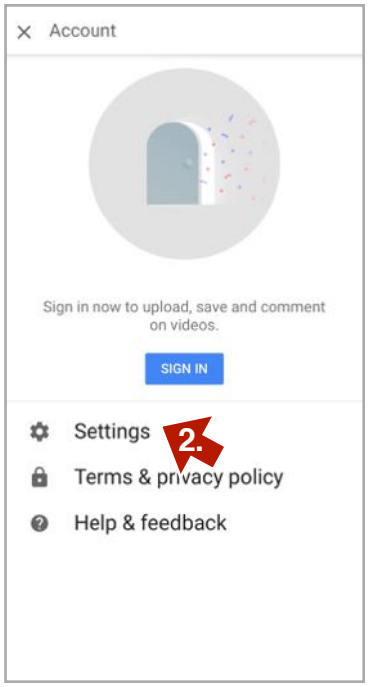
YouTube Safe Search Apple Mobile App

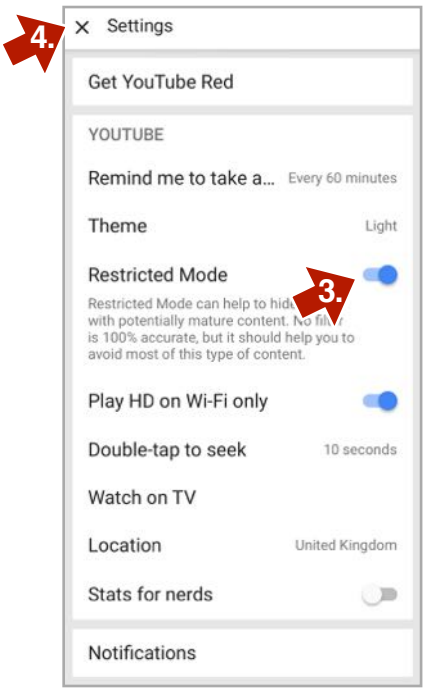
Open YouTube Mobile app - 1. Click profile, top right. 2. Go to Settings menu. 3. Click “Restricted Mode Filtering” to the on position. 4. Click X to exit.

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.

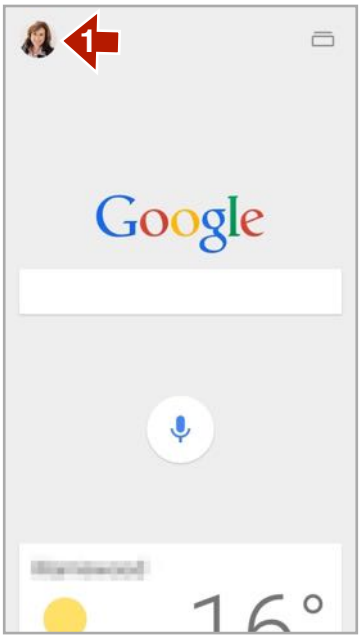


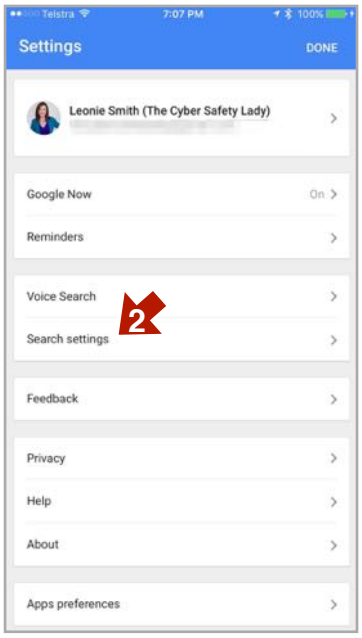


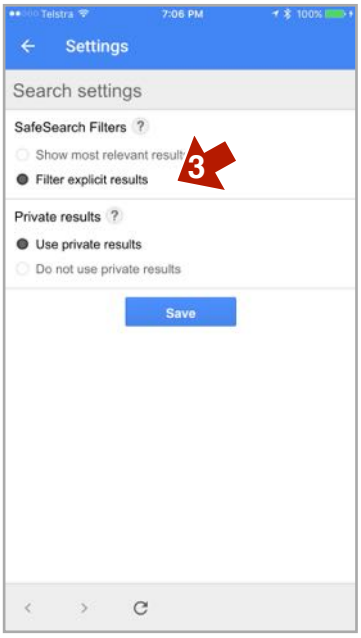


Google Safe Search Apple Mobile App

1. Open app. - Go to profile. 2. “Search Settings” 3. Click “Filter explicit results”. Click Arrow back to exit out. Set Safe Search on all Browsers and Google apps. For PC settings see P.19
   Note: Cannot be locked on with a password







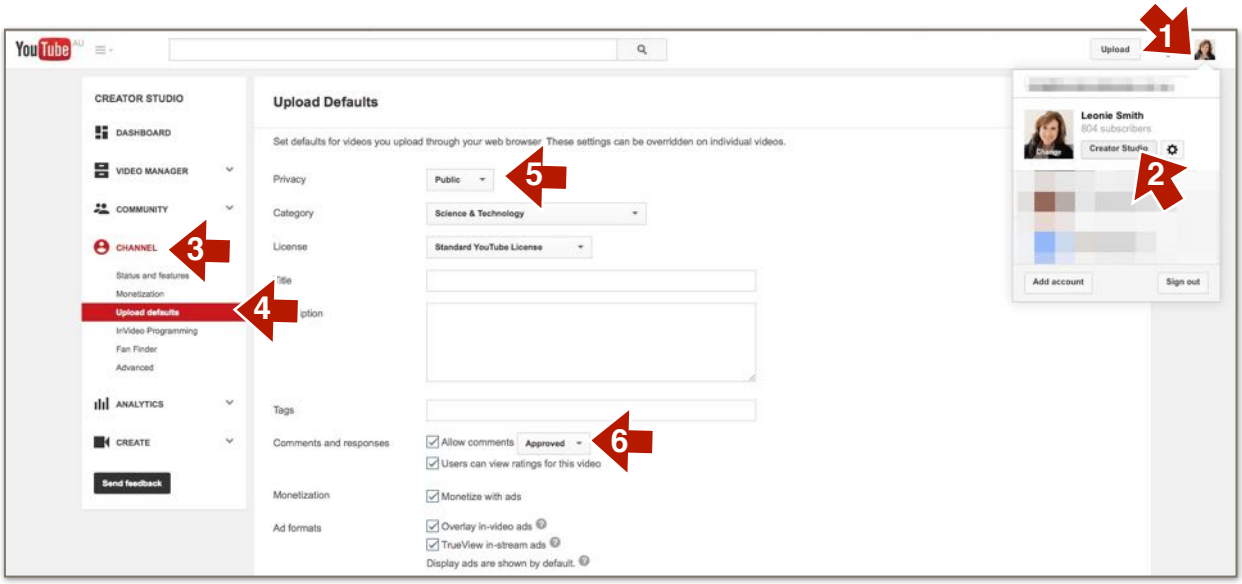
Android: Open Google Mobile app. “Settings” - “Privacy & Accounts”. Scroll down to “Safe Search Filter” and enable.

YouTube Channel Privacy Settings - PC - Laptop

Creator Classic view - switch between YouTube Studio Beta in settings

Private Channel. Log into the channel you wish to make private.

1.Go to channel profile. 2.“Creator Studio”. 3.“Channel”. 4.“Upload defaults”. - 5.Change “Public” to “Private”. Un-tick “Allow Comments” if you want to block all comments. 6.Or change “All” to “Approved”, to approve comments before publishing.

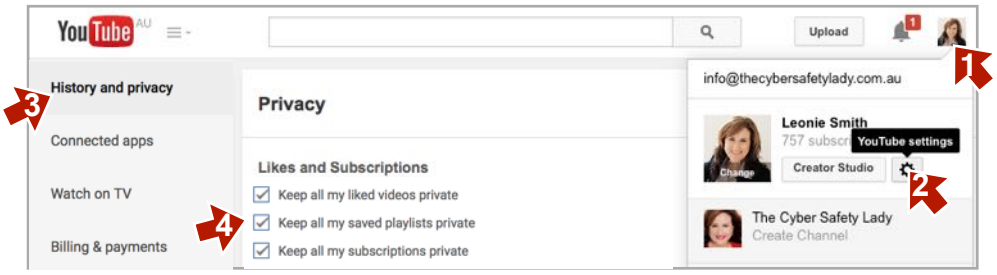


Hide Your Likes And Subscriptions

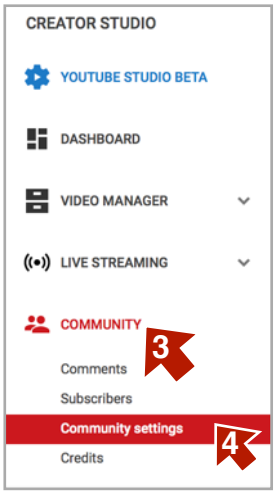
Log into the channel you wish to apply these settings to.

1.Click Channel “Profile pic”. 2.Click “Settings wheel” (YouTube Settings).

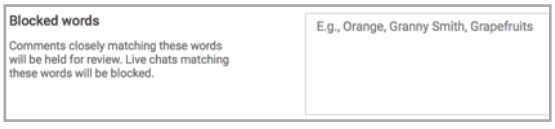
3.“History and Privacy”. 4.Tick the privacy options you require. Click Save



Control Comments And Blocked Users



Click on 1.”Profile pic”. 2.”Creator Studio”. 3.Scroll across to the left column to “Community”. 4.Scroll down to “Community Settings”. Scroll down to “Default settings” and set comment preferences as needed. You can blacklist swear words here also for extra filters.

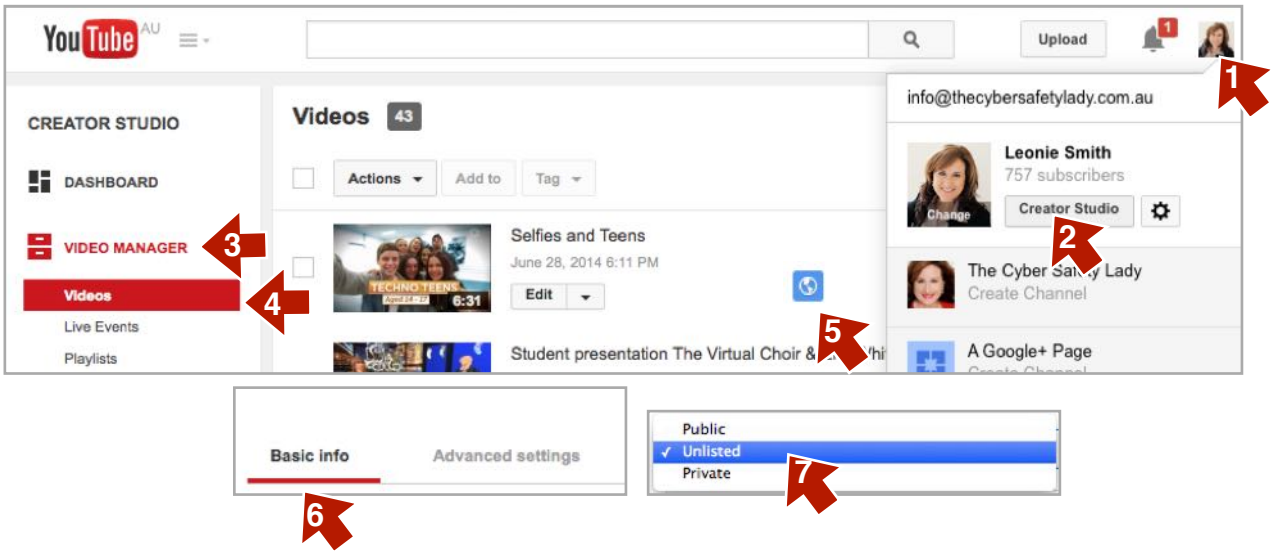


Add or remove hidden YouTube users also on this page. To hide users, use the flag menu on the Comments page.

To Set A Video As Private

Log into the channel you wish to apply these settings to.

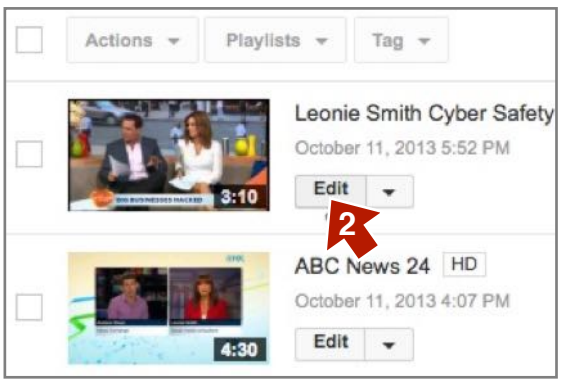
1. Click Profile pic. 2.“Creator Studio”. 3.“Video Manager”. 4.“Videos”. 5.Click the blue globe icon to the right of the video. 6 to to basic info. 7. Select “private” or “unlisted” from next window, (located lower right in “Basic Info” settings) Click “Save Changes”. **Note:** You can set the privacy options whilst uploading your video, when filling in your video’s title and other information.

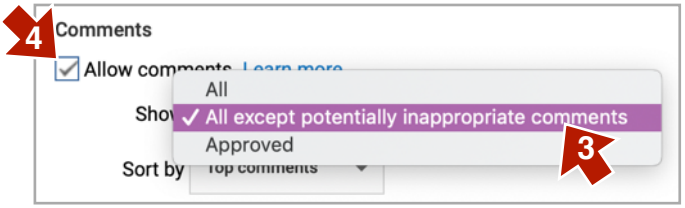


Disable Commenting On Your Video

Commenting on YouTube can be used for bullying.

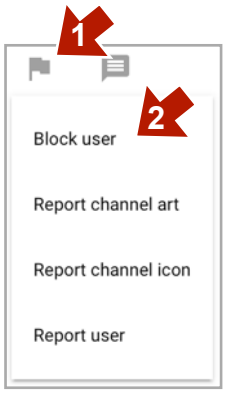
1. Go to “Video Manager/Videos” as above instructions.
2. Select “Edit” on the video.
3. Under your video go to”Advanced Settings”.
4. Un-tick “Allow Comments” or set to “Approved” or “except inappropriate”.



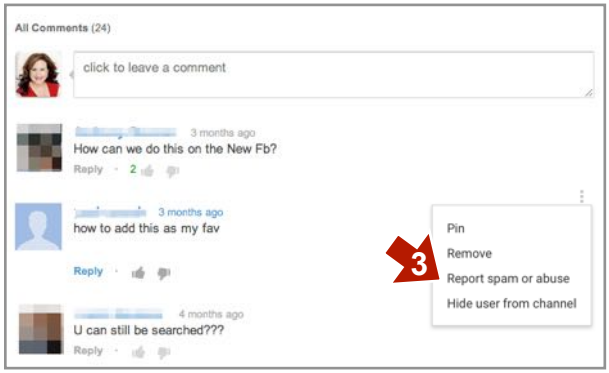


How To Block Another YouTube User

Block by going to the users profile then
1. Then click the flag icon. Click “About” To find flag if not showing.
2. Select “Block User” or “Report User”



3. Or block/report them via their comment under your video. Find drop down menu (three vertical dots) far right of the comment select “Hide User” or “Report…”

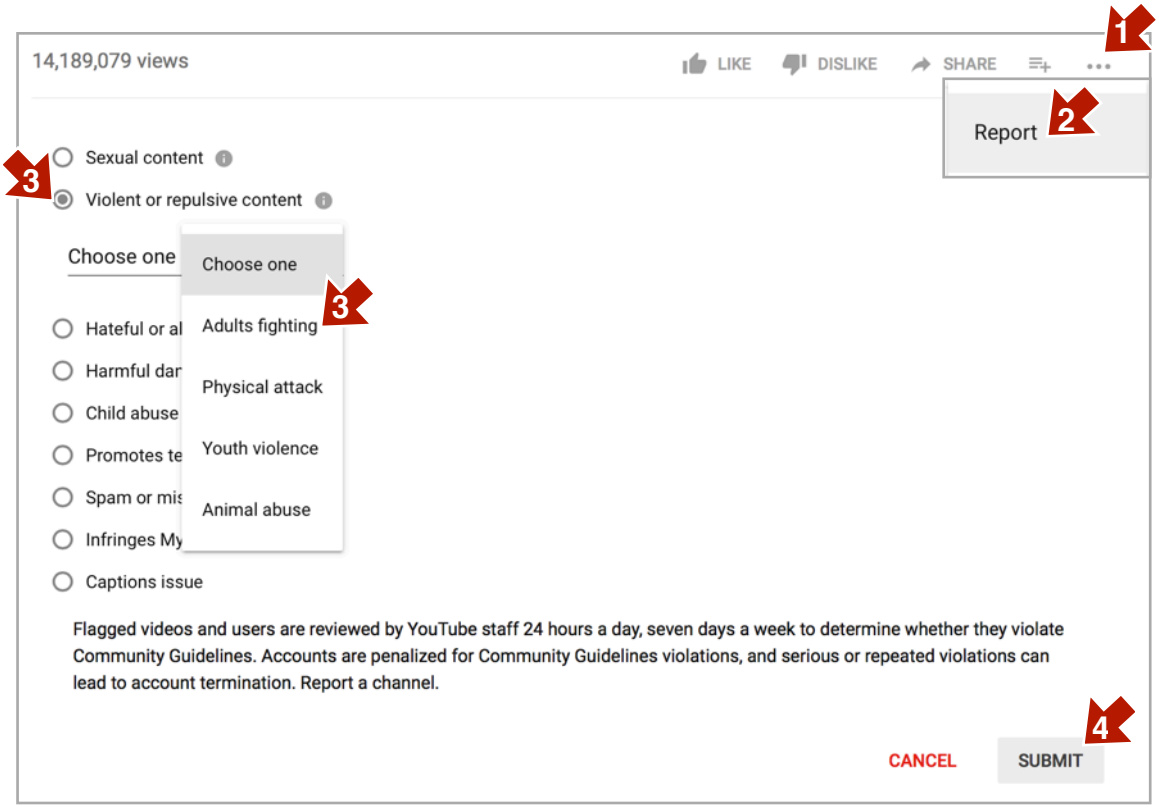


Mobile YouTube: Go to their profile - click the 3 vertical dots icon, top right next to search icon to select “Block User”. Or click the 3 vertical dots next to their comment and select “Report”

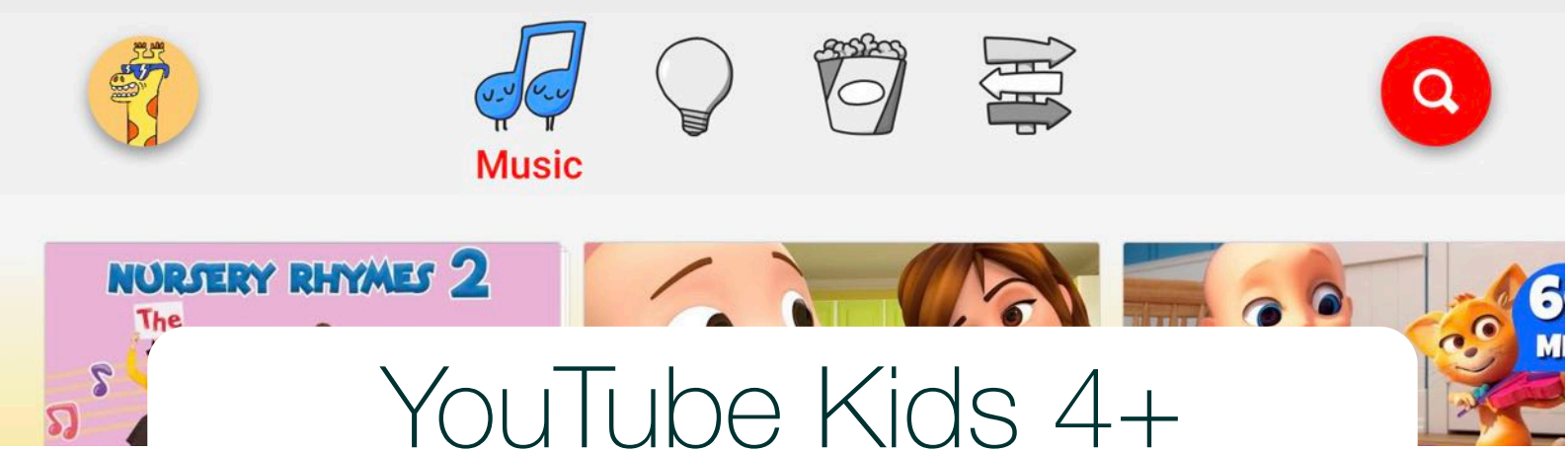
Report/Flag A Video

To report a video as offensive or to have it removed, navigate to beneath the video.

1. Click “… More” 2. “Report” 3. Select the reason. 4. Click “Submit”. YouTube will remove the video if it violates their community guidelines.



For mobile Y.T app, click 3 vertical dots top right of video, click “Report”



YouTube Kids 4+

"YouTube Kids" rated age 4+ now has more parent controls to prevent your child seeing inappropriate content. The content on YouTube Kids can be too scary for younger children, and may contain media you don't want your child exposed to, including talk shows, rock music, Tween type shows, cartoons with violence, or strange themes. It is highly advisable to enable the full parental controls for children under 8 years of age.

Parental controls are not a substitute for close parental supervision
Please make sure you sit with your younger children and watch YouTube with them so that you can share in their experience and answer any questions about what they are viewing. You can set up YouTube kids on your smart TV so that you can supervise much easier than on an iPad, by streaming YouTube Kids from a mobile device using Chromecast or Apple T.V. There is no parental controlled YouTube Kids app yet for Smart TV's or Apple T.V .

To use the full parental controls in YouTube Kids you must have a Google account.

Moderate Your Child Viewing
You can now select the shows you prefer your child to watch and set YouTube Kids to only show those shows, or channels. It is safer for you to moderate and choose the shows you would like your child to see rather than rely on YouTubes suggestions. If you don't recognise the show, it is advisable to watch a few episodes to see if you think it is suitable for your child, or choose only shows you already know and approve of. Be sure only to choose high quality genuine productions.

Setting up your child's profile
You can create up to 8 seperate child profiles on the one app/device. Your child then selects their own personalised profile when they open the app. You can also passcode protect each child profile to ensure children don't use the incorrect profile, or switch profiles. If you have set a viewing timer on their profile for a session, they could switch profiles if passcodes are not set for each profile, and continue watching on another child's profile. So individual profile passcodes that only parents know is advisable. See step by step video Here or scan the code.

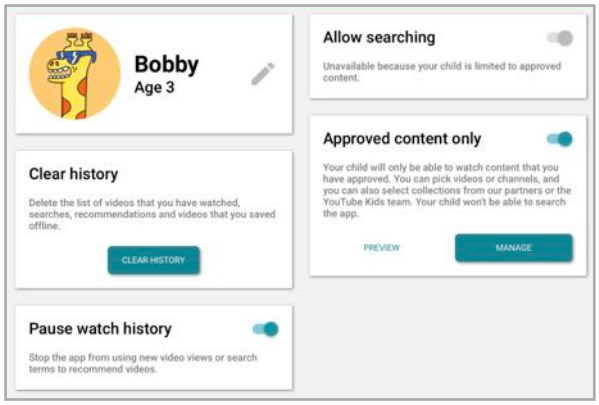
1. Click the profile Pic or Lock icon
2. Input the year of your birth or create a password
3. Sign into Google with your account
4. Click the + sign to add a child profile, enter your Google password
5. Create your Child's profile name and enter their Birth Month/Year
6. Turn "Search Off" on next screen. It is safer for children not to search for new content.
7. You can then add other children's profiles.
8. Click the Lock icon to adjust settings as you require

To change the settings in your child's profile you will need your 4 digit YouTube Kids parental control passcode and the password for your Google account.

Go to the profile of the child you wish to set. Click on the lock icon (lower right) - put in your 4 digit parental control passcode and click settings. Again select the profile you wish to set, enter your Google account details.

Once in the settings of your child's profile ensure that (see pic below)

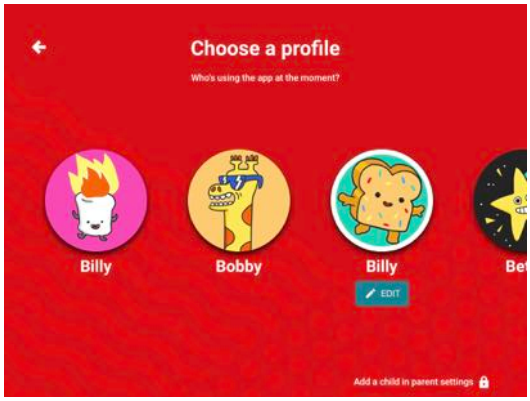
1. Set "Allow Searching" to the off position to prevent searching for content within the app
2. Set "Approved content only" to the right - on position
3. Click "Start" or "Manage" to select content
4. Click through the top icons to select "Collections" or "Explore" or "Music" or "Shows" or "Learning" select programs or channels as you go.



5.Click the small + top right of each show panel to add those channels or shows to the approved list for your child's profile.
6.Preview the shows by clicking the panel to see what shows are included before adding, each panel may have multiple shows.
7.Click "Done" to set
8.Also Set "Pause Watch History" to prevent suggested videos showing up.
9.Exit back to login screen and check the profile to ensure it is set as required.

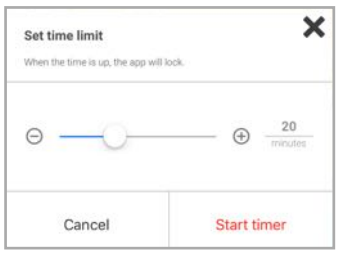
Important! To prevent your child watching other content or extending time limits.

Set seperate passcodes for each profile, so that children cannot switch profiles. Each child can have possession of their own code, or you can set it so that only you the parent knows their codes. This stops children from switching profiles to avoid timer settings or watching videos for older children. For added security make sure your child doesn't know their code to prevent logging out and re-logging in to extend time.



1.Click the profile icon you wish to set a passcode for
2.Click the "Edit" button under the profile pic to go to "My Settings"
3.Click the settings icon top right of screen
4.Click "Create Secret Code", set a 4 digit code
5.Click "Got It" to set
6.If you forget the passcode you can reset it via "Edit" and "My Settings" for that profile

Setting the YouTube Kids built in timer to limit screen time



Parents can also set a timer so that the app shuts down after a set time. After setting the timer, a popup at the bottom of the screen will notify the viewer of how much time they have left to watch. When viewing time is up the screen changes to a static picture (see below). Note: If your child knows how to switch profiles (if there are no profile passcodes set) or knows how to log out of the app, by double tapping the home button and swiping the app up, they can bypass the timer so beware! Setting each profile with a parental lock code that only you know, is a more secure way to prevent your child from logging back into their profile after logging out when the timer is up.

1. Tap the lock icon in the bottom corner of any page in the profile you want to set a timer on
2. Enter your parent custom passcode
3. Select “Timer"
4. Use the slider bar or - and + icons to set time limit.
5. Tap “Start Timer”
6. Kids will get warnings as to how much time is left and then see a "Time's up!" notification when the app will be frozen.

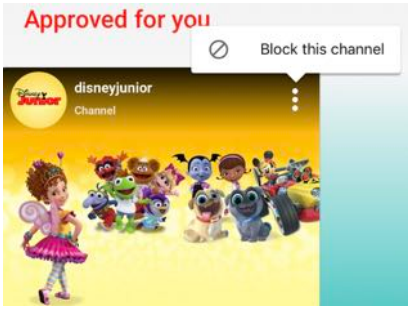
The profile will need your parental password to be enabled again.

To unlock the screen and reset timer -

1. Tap the lock icon in the bottom corner of the profile you wish to enable.
2. Enter your custom parent passcode
3. Select Timer, then extend the time or tap “Stop” or “Exit Timer”

Blocking Videos

You can block or report any videos you don't want your child to have access to by clicking the 3 vertical dots on the top right of any video window or panel.



Coming Up!

The parental controls on this version of YouTube Kids may change in the future. YouTube have introduced a new two tiered approach to YouTube Kids to make it easier for parents to navigate. One profile type will be for younger children 8 years and under, the second profile type will be for “Tweens” 8 years to 12 years old. Right now these profile types are only available in the U.S., but may be introduced to more locations in the future.

A Premium Version Of YouTube Kids

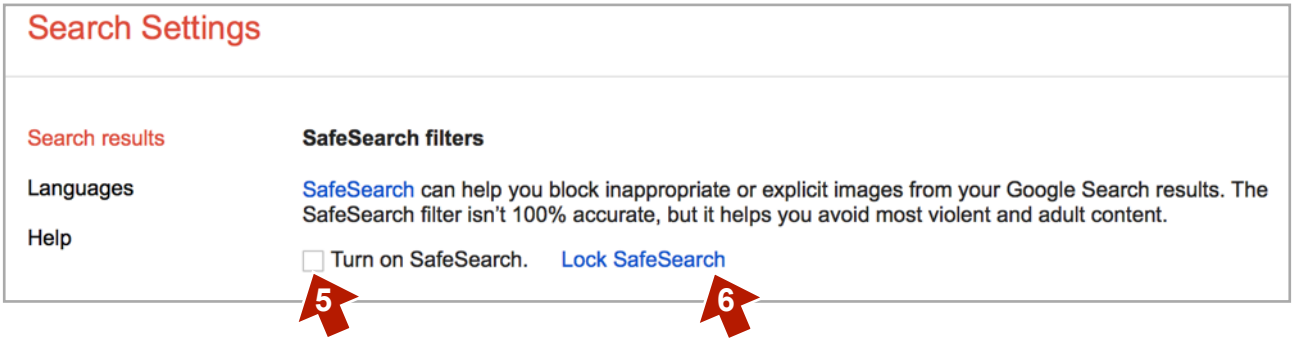
You can limit the advertising in YouTube Kids, and also download videos for watching offline, by upgrading your account to the pay for YouTube Premium, then enabling it on YouTube Kids. More Here https://support.google.com/youtubekids/answer/7030713

Find more information on YouTube Kids Here https://support.google.com/youtubekids

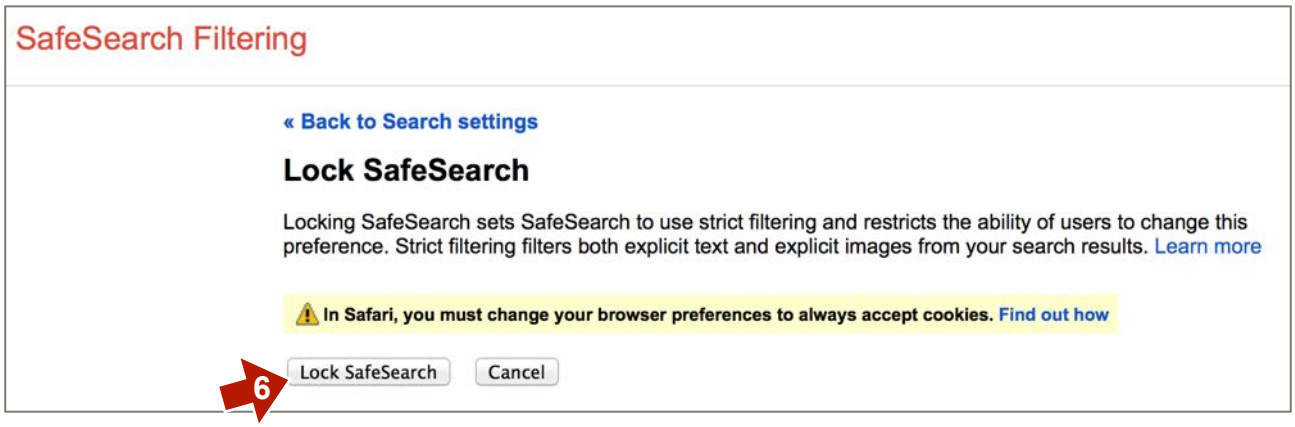
Google Safe Search Settings for PC - Laptop

To prevent adult content showing up in search results, these settings must be applied to every browser on every computer, and on every mobile device browser your child uses. See Page 15 for mobile settings.

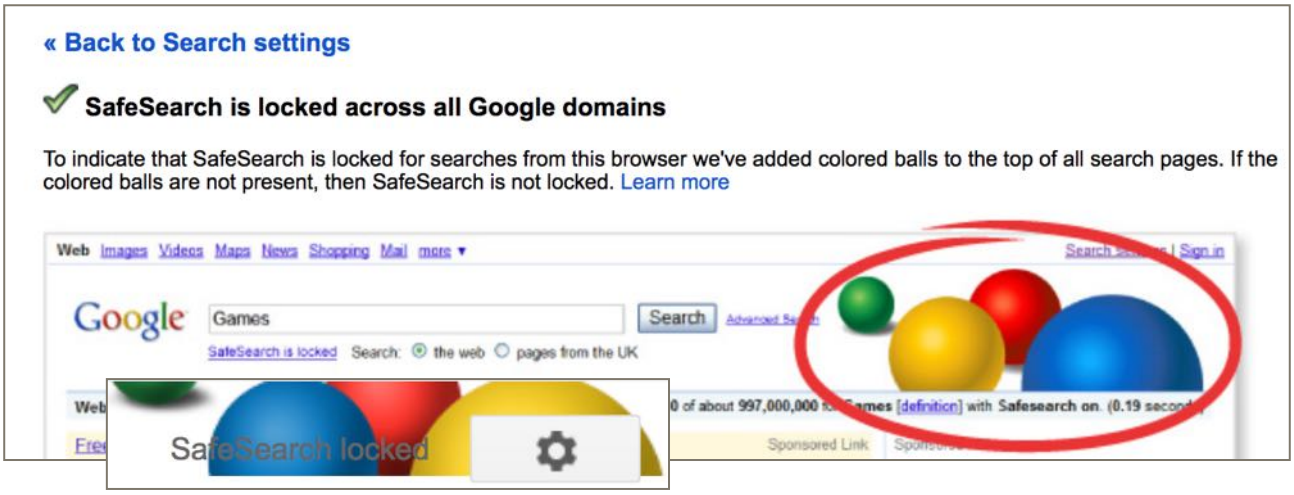
1. Enable cookies in your browser Microsoft Edge: 3 dots top right/Settings/Advanced Settings - Scroll down to “Don’t Block Cookies”. For Safari/Preferences/Privacy/Don’t Block Cookies. Chrome/Preferences/Show Advanced Settings/Privacy/Content Settings/Allow
2. Make sure you have a Google account, sign up if not.
3. Log in to your Google account.
4. In the browser address bar type in http://www.google.com/preferences
5. Tick the “Turn on SafeSearch” box



6. Google will ask for your password again. Sign in, then click "Lock SafeSearch".

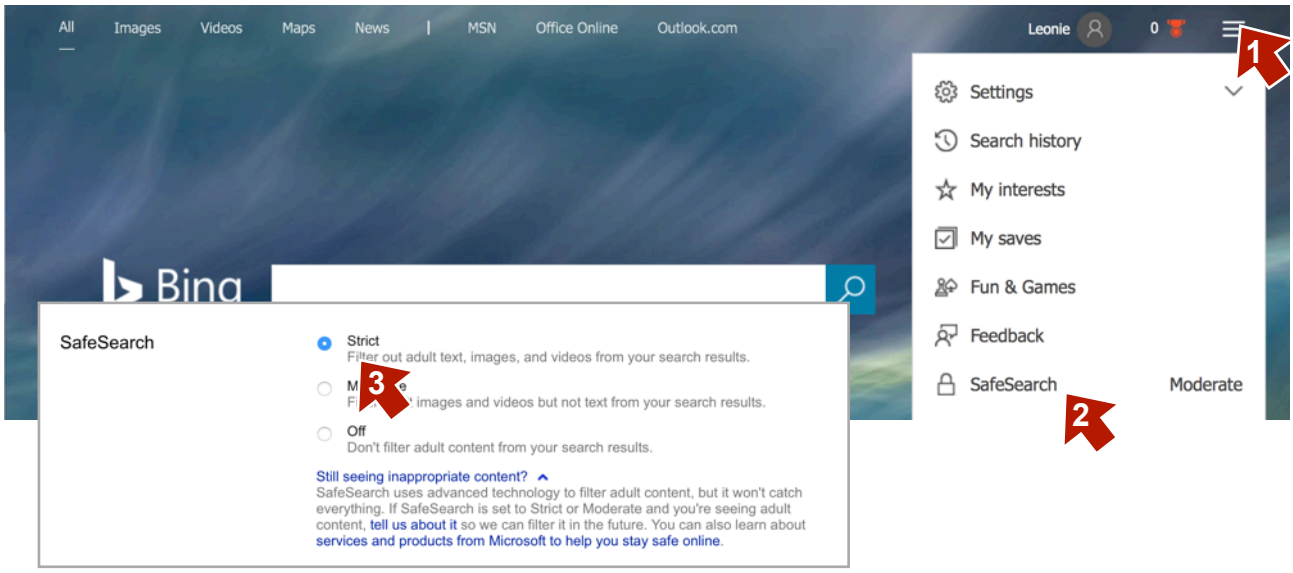


7. You will then see these coloured balls top right side of Google "Search" (not visible on mobile device) indicates this browser is protected by "Safe Search". Reverse procedure to unlock. Log out of your account, the browser search is now safe search locked.



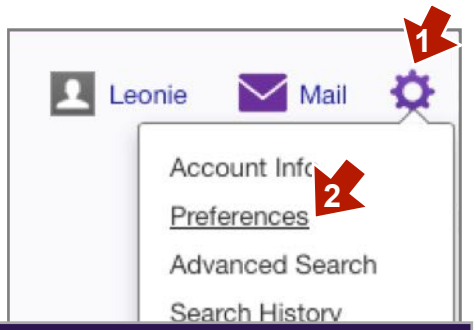
Safe Search For Bing - PC - Laptop

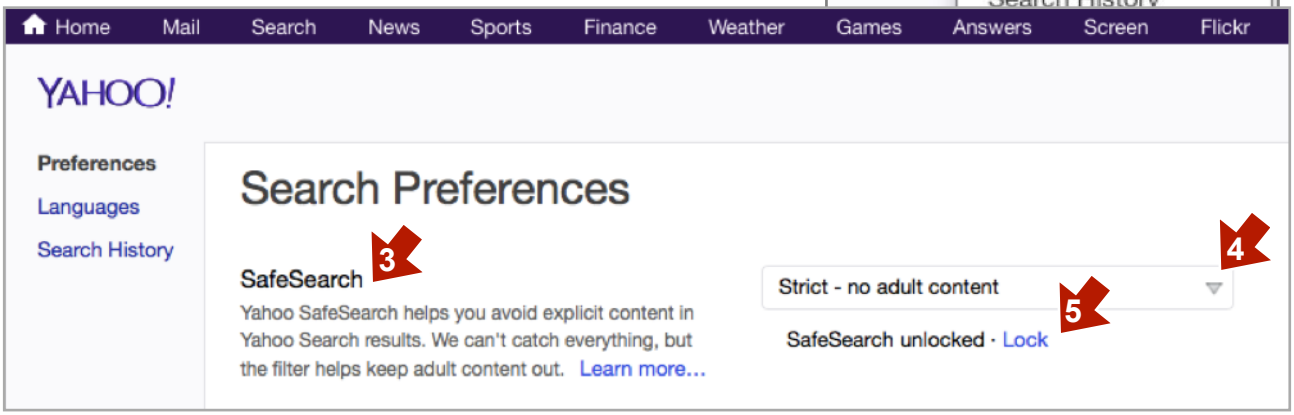
Bing search is the default search engine for the Edge browser. Open the browser app and then http://www.bing.com Go to top right of the page and click the 1. “Menu" then scroll down to 2. “SafeSearch” 3. Set to “Strict" or "Moderate" according to the age of the child.



Yahoo Safe Search - PC - Laptop

1. Sign in to your Yahoo account.
2. Navigate to http://search.yahoo.com/preferences .
3. Scroll down to “SafeSearch”.
4. Set to “Strict” or “Moderate” and then save.
5. Click “Lock” to secure.





Private Messaging App Dangers

The biggest danger with messaging apps for younger children is unsupervised conversations, bullying, sharing adult content, sexting and risk of contact by strangers.

Some messaging apps encourage the user to share their user name to social media platforms and to sync their devices' address book. This is a danger for children due to the extra exposure.

Set Privacy Settings To Block Stranger Messages: Not all messaging apps have secure privacy settings, so children may be sent messages directly without a friend request. Instruct children never to accept unknown friend or message contact requests or to answer calls or messages from unrecognised numbers or contacts.

Warning: Kik Messenger allows anonymous unverified accounts which means it is very hard to trace users if something goes wrong and the police need to be involved.

Note: The safest messaging apps for children are ones with privacy settings that actually block messages from reaching your child, where they only get contacted by people they know.

Don't Use Real Names: Ensure your child sets up messaging or gaming accounts with pseudonym user names. Make sure they share user names only with approved friends.

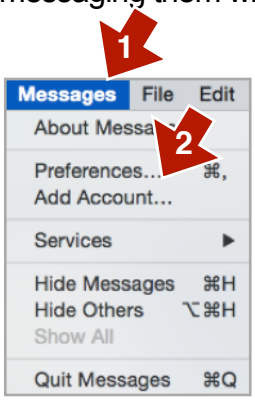
Tip: Share a Skype or iMessage account with your younger child to supervise messaging in real time. This way you can see the messages and chat whilst it is taking place. Do let all participants know you are supervising including parents of your child's friends in the chat. Facebook Kids Messenger was not released in Australia at time of publication.

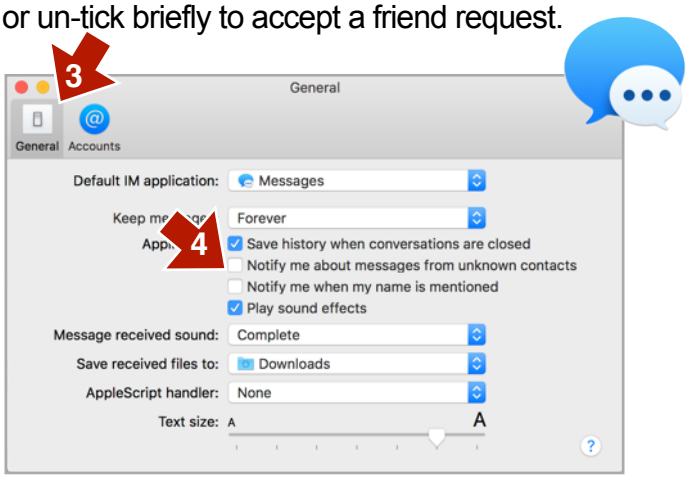
To delete a Kik Messenger Account - Tap "Settings" - Select Your Account - Tap "Log Out" go to https://ws.kik.com/deactivate and enter the email address registered with the app. They will then send an email with a link to deactivate the account.

Supervision is very important when children are first starting to use messaging apps. Make sure all participants in the chat know that mum or dad are supervising for reasons of full disclosure and respect for privacy

Apple Messages Privacy - for PC or Laptop

To hide messages from unknowns on iMessage (Apple Messages) set privacy settings. On a Mac PC open the app and go to 1.“Messages” (top left menu). Then to 2.“Preferences” - 3.“General”. 4.Un-tick “Notify me about messages from unknown contacts”. Add new friends by messaging them with a friend request, or un-tick briefly to accept a friend request.



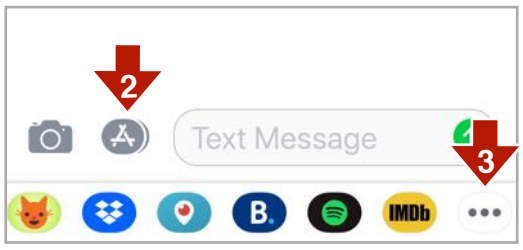


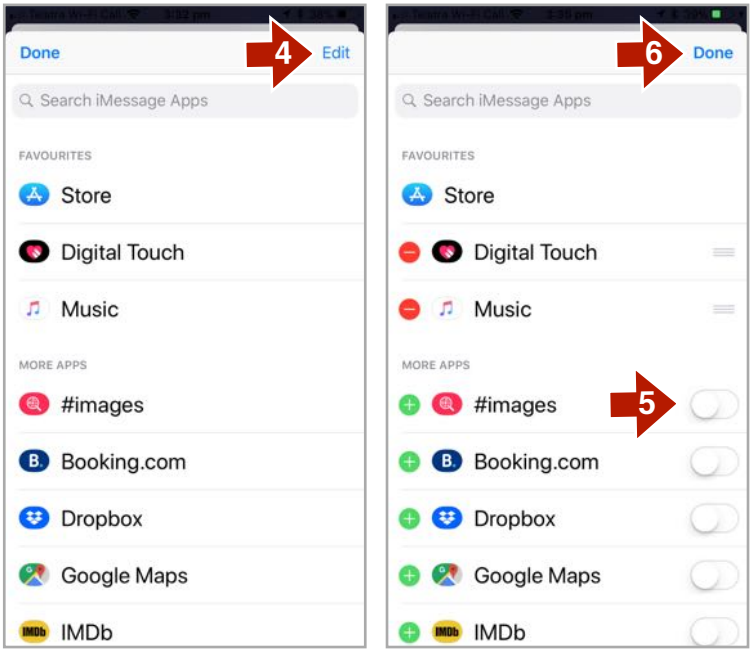
Messages Apple Mobile Set privacy on mobile iMessage via Device “Settings” scroll down to “Messages” and click. Then scroll down to “Filter Unknown Senders” set to the On position (green). Exit out of settings to save.

Blocking Gifs & Extension Apps: via Apple Messages mobile app

Apple iOS10-11 Messenger has Gif’s, images & add on Apps. Some may have adult content.

1. Open a previous message in Apple’s Messenger App.
2. Click the A symbol. (see below) to bring up the extensions menu if not showing.
3. Scroll extension menu to the left and then click 3 dots bottom right.
4. Click Edit (top right) to disable any extensions and #images app.
5. Set toggle buttons to the left (White) of any apps you wish to disable in Messenger.
6. Then click Done and exit out.





Important: To prevent #images being re-enabled. Go to Settings/General/Restrictions/Installing Apps and slide toggle to the left to disable. iOS12 Settings/Screen Time/Content and Privacy Restrictions/iTunes and App Store Purchases/Installing Apps/Don’t Allow exit back

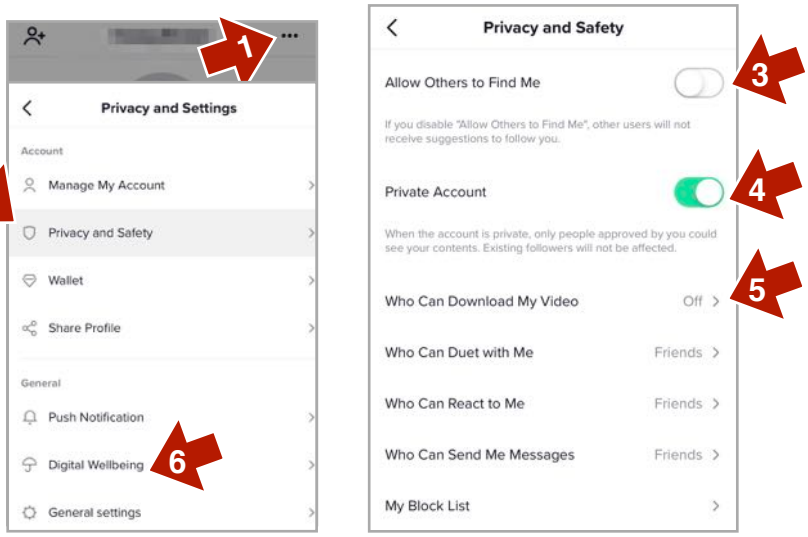
musical.ly TikTok Privacy Settings

musical.ly (now known at Tik Tok) is a video sharing app. Rated13+yrs due to adult content and public social media aspect. Tik Tok has important privacy settings to prevent you posting your video to the public, there are risks of bullying, adult followers and misappropriation of your content. It has “In App Purchases or “Coins” Some young users have spent thousands of dollars on coins. Report any inappropriate videos or nasty comments using the report features.

To set privacy settings:

Go to your profile icon lower right of home screen.

1. Click the settings … menu
2. Select “Privacy and Safety”
3. Set “Allow Others to Find Me”, according to preference, off is safer.
4. Enable “Private Account” set to on.
5. Set download to off, duet, react, and messages to Friends.
6. Set a time limit on your use, filter adult content.



Hide your location through your phones privacy settings. Settings/ Privacy Location Services/musical.ly

Beware: Allows live video streaming to a live public audience. Public live video can attract bullies and creepy people.

Instagram Privacy Settings

Privacy Settings:

1.Go to your profile page.

2.Click on the menu

3. Scroll down to “Settings” menu then scroll down to “Account Privacy”

4.Enable “Private Account”.

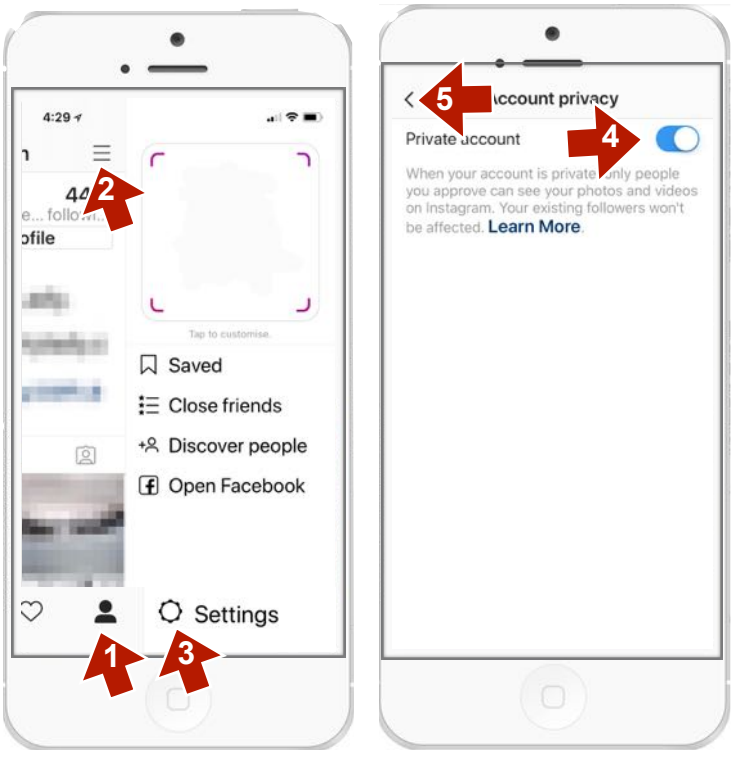
5.Go back & set all options to safest settings.

Filter inappropriate comments or keywords in “Comment Controls”

Two-factor Authentication prevents hacking. Use an Authentication app like Google Authenticator, not phone number. Keep ph numbers offline.

Story Controls: Select audience for stories and message settings. Turn off sharing.

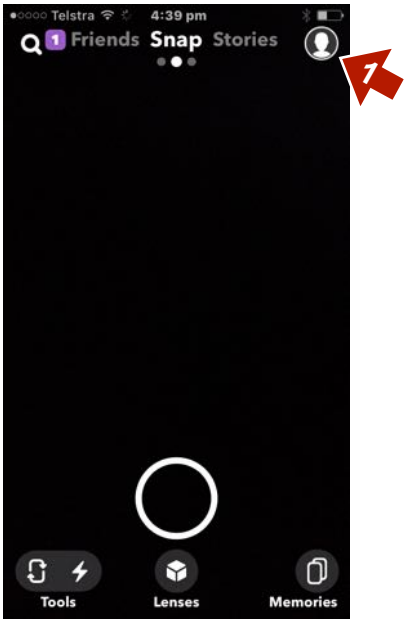
Location Services: Disable through phone settings - Privacy - Location Services - Instagram - set to “Never”.

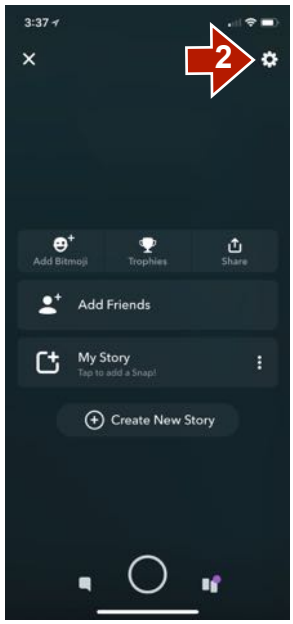


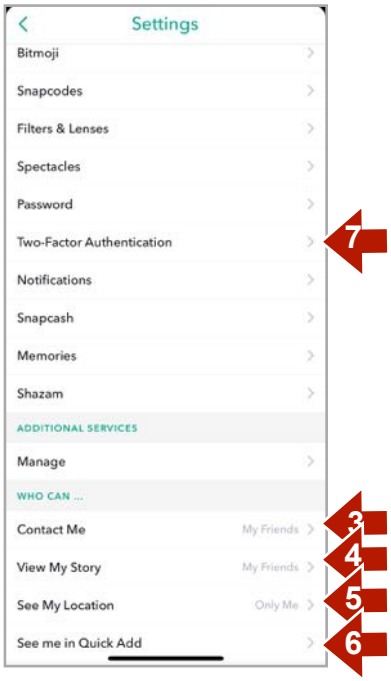
Snapchat Privacy Settings

Snapchat is advertised as a messaging app where messages “disappear”. However Snapchat photos CAN be screen-shot, saved & shared. Using the new feature “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.

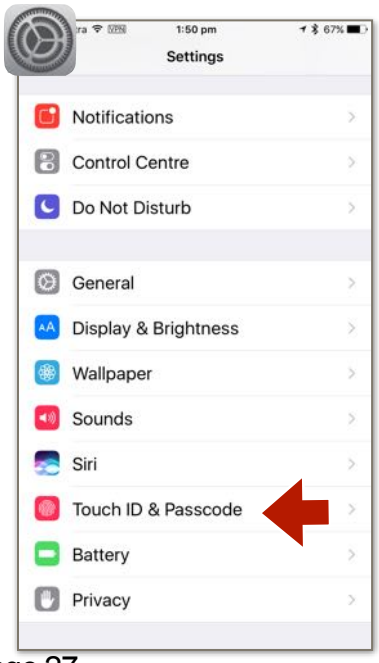


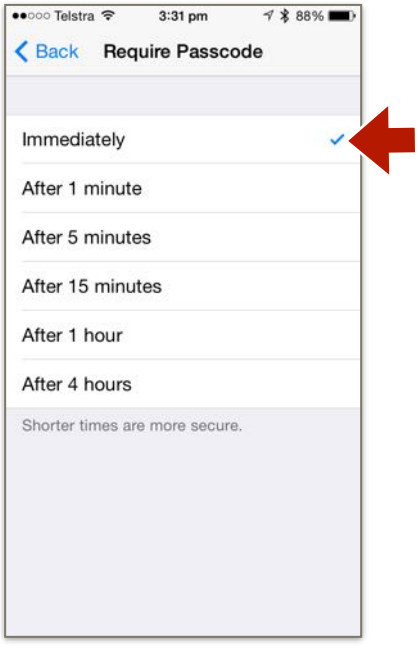




Setup Screen Lock On Apple Mobile

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 has Face ID & Passcode settings.

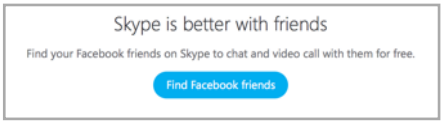




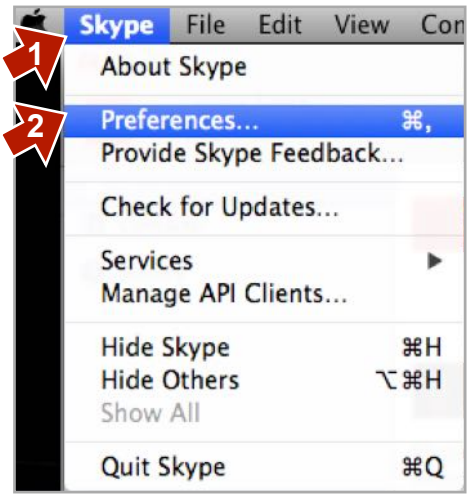
Skype Privacy Settings Mac P.C or Laptop

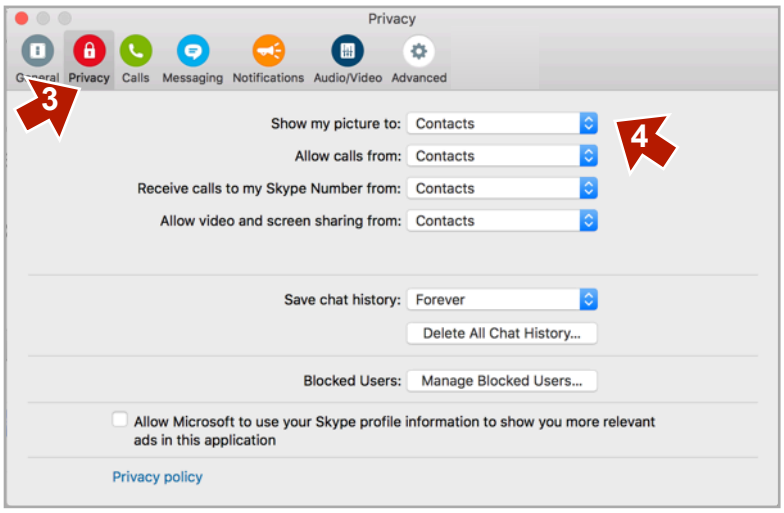
Skype has a proven history of safety if setup with privacy settings and your user name is kept private, only give it out to trusted contacts. For children and teens it is best to create a “made up” user name for extra privacy. Be careful using a webcam, it may give away private information about you. Students and children should report any messages or friend requests from strangers to adults and block. Sharing an account with younger children can help parents to supervise use. Parents and child can be logged in at the same time. These privacy settings are account “Cloud based” (no need to set on every device).

Note: Make sure you do not connect Skype with Facebook contacts, as per the prompt. See pic ⇨



1. Open Skype App and click “Skype” Menu
2. Click ”Preferences"
3. Click on "Privacy"
4. Change all to "Contacts" as below

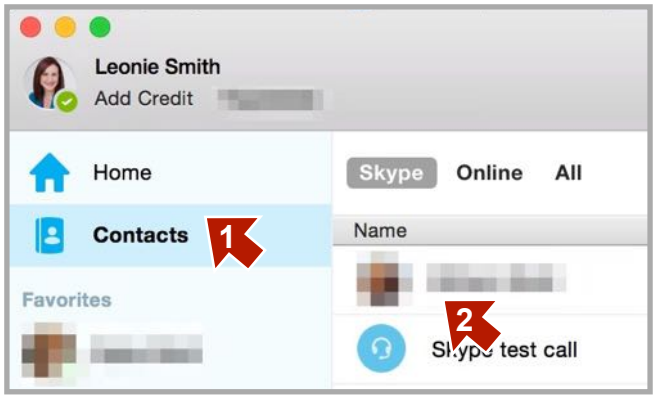




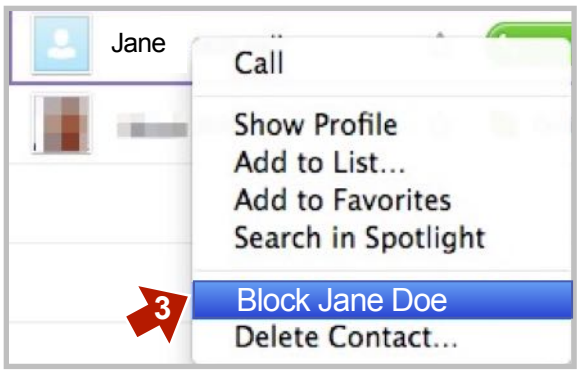
Note: Do NOT accept friend requests from people you don’t know. Click decline and block if necessary. Don’t sync your address book with Skype. Add your friends one by one.

How to Block A Contact

Go to 1. “Contacts” menu in left column.
2. Scroll to locate the contact you wish to block.



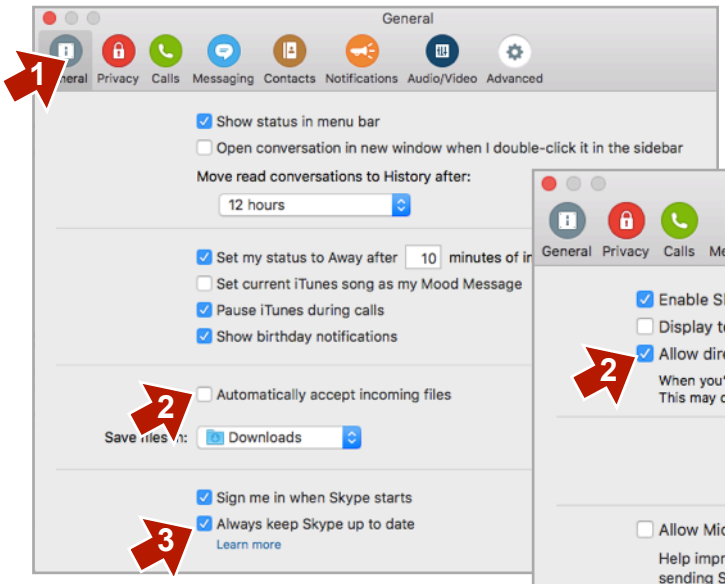
3. Right click on contact name and select the “Block” option from drop down list. Or on Mobile go to profile (hold finger on name) and scroll down to “Block contact”



Skype Security Settings Mac PC or Laptop

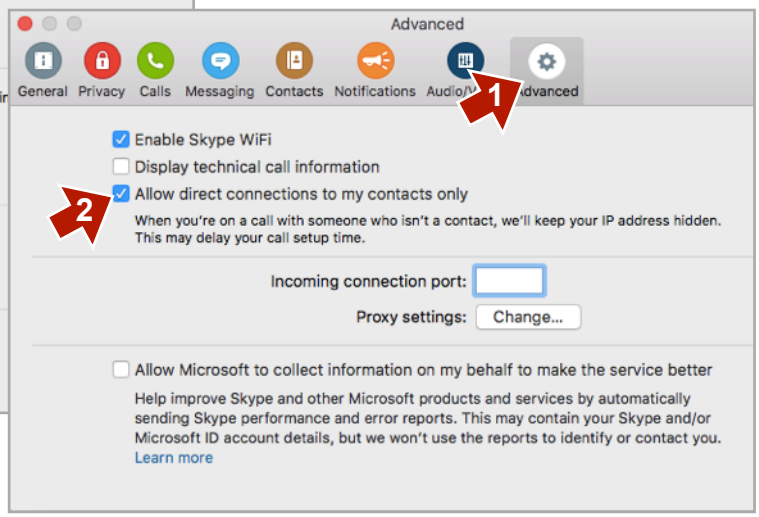
To help protect against receiving a virus or unwanted content via a Skype message, you should set Skype so that it doesn't automatically download files to your computer.
Go to your Skype preferences as per previous instructions.

1. Click on "General" Menu
2-3. Scroll down and un-tick both settings as per below picture.



For extra Security Set Advanced Settings as below

1. Go to "Advanced" Menu
2. Tick "Allow direct connections etc…"



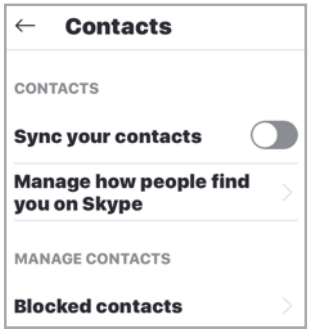
Mobile Skype

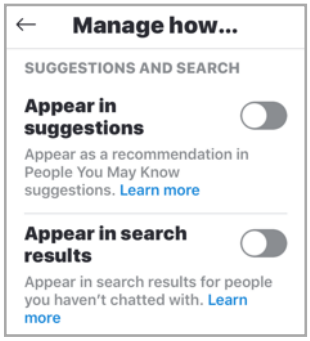
Privacy Security Settings:

Apple Mobile Skype: First open Skype

1.Click your profile picture - top/centre
2.Click settings icon far top right.
3. Scroll down to Contacts and Manage how people find you.

Don't sync contact, but add contacts manually and carefully.





To Block:

1. Go to the name of the profile you wish to block.
2. Click their name top left to open full profile
3. Scroll down and click "Block Contact" Report Abuse if necessary.

Android Mobile Skype: First open Skype

1. Go to "Settings"
2. Under "Contacts" Set "Don't Copy Contacts".
3. Under "Privacy" - Set "Allow IMs From" and "Receive Calls From" to "Contacts Only."

To Block:

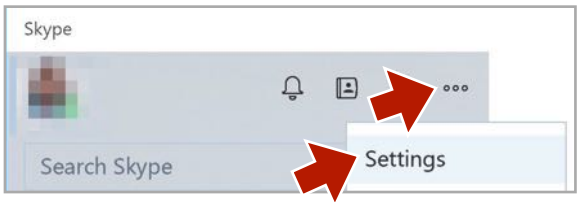
1. Go to the profile of the person you wish to block. 2. Click "Settings" via 3 dots top right 3. Select "Block Contact" from menu

Skype Privacy Settings Windows 10

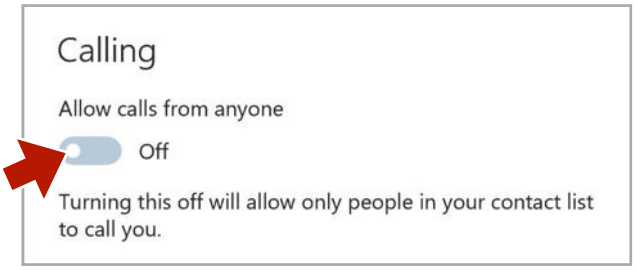
Prevent random strangers from sending you a direct message.

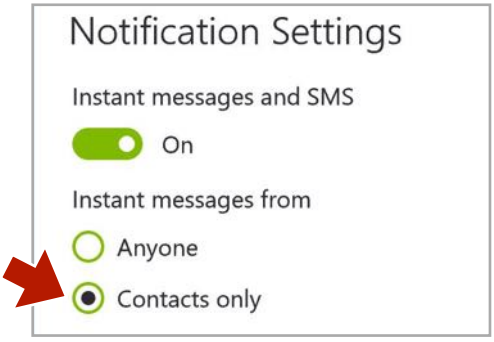
Use a made up name for extra privacy. Set the privacy so that only approved contacts can message you. Decline friend requests from people you don't know. Block if necessary.

1. Go to … more menu top Right - click "Settings" from drop down menu.

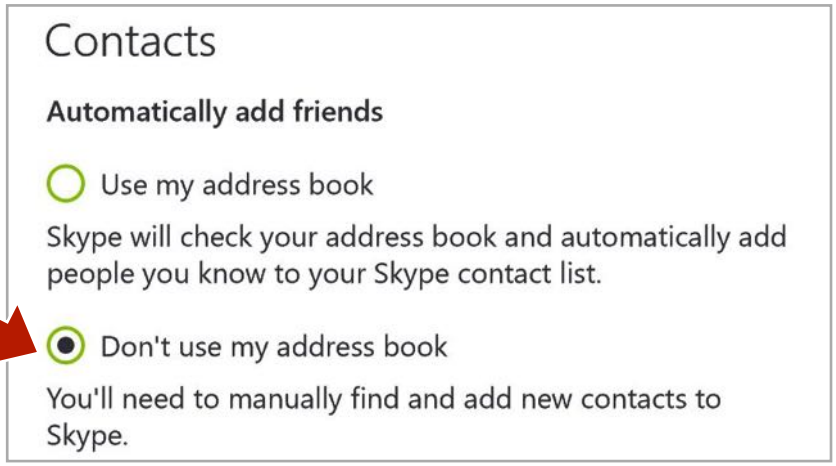


2. Set all contact/calling and notification settings to Contacts only.





3. Avoid Syncing your address book with Skype. Add contacts manually as you need them.



Blocking:
Right click on the profile name of the person you wish to block and click "Block This Person".

Children & Teens should tell an adult they trust if they have been sent messages on Skype from someone they don't know.

Note: Some people have been using "Voice Changers" over Skype and other voice apps to pretend to be someone they are not. Don't trust a voice to determine if your Skype "Friend" is who they say they are. Adults can pretend to be younger, men can pretend to be women

Facebook Privacy Settings

To Find Out What You Are Sharing Publicly For Facebook on computers

Go to your profile 1. Click “View As” on cover picture. **(Oct 2018: this option may be missing, Facebook disabled it after a recent hacking event - hopefully it will be restored)**

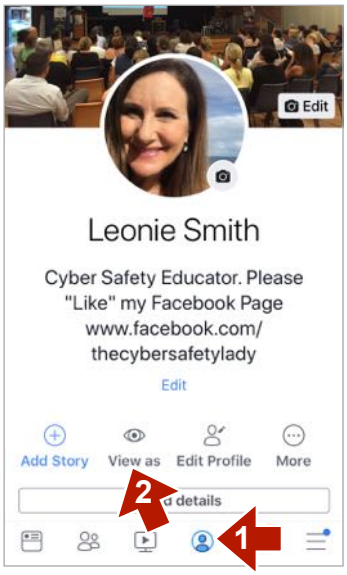
A truly private profile should only show your name, cover and profile picture, no posts or groups or other personal info or “likes”. You can’t hide your profile pic or cover pic, but set them carefully with an eye to privacy. Go through all the tabs to check what is showing, then exit out of “View As” and change and delete anything you don’t want public. Check back to “view as” to see if you have deleted/changed enough.

2. Hide all your personal information posts and photos through the “About” or “Edit Profile” menu and set all your personal information, including your relationship status, your likes, your location and employment to “Only Me” or “Friends Only”. Delete any information or posts you don’t need to share.

Don’t Leave It All Up There. Hacking happens. Delete your old posts occasionally for better privacy. Delete/hide old profile and cover pics from your photo albums. Go to “View Activity Log” and delete your old posts one by one. Unfortunately there is no “Delete All” button.

Note: Facebook settings are cloud based, setting them on your computer or mobile device will set them across all your devices.

No personal information, posts or photos.



The Mobile version of Facebook (see left pic) now has the “View as” setting available from your profile page.

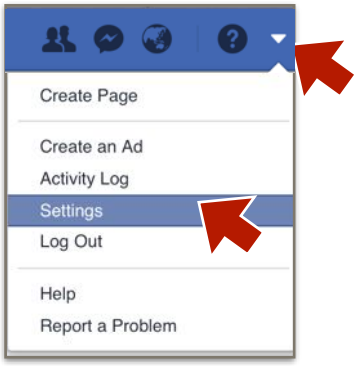
1.Click the profile icon - bottom menu - to go to your profile page.

2.Click the “View as” link.

Go through each tab - About - Photos - Friends, to see what is showing.

To edit your content exit out of “View as” click back arrow, and delete and hide your data as needed.

Facebook Privacy Settings P.C or Laptop

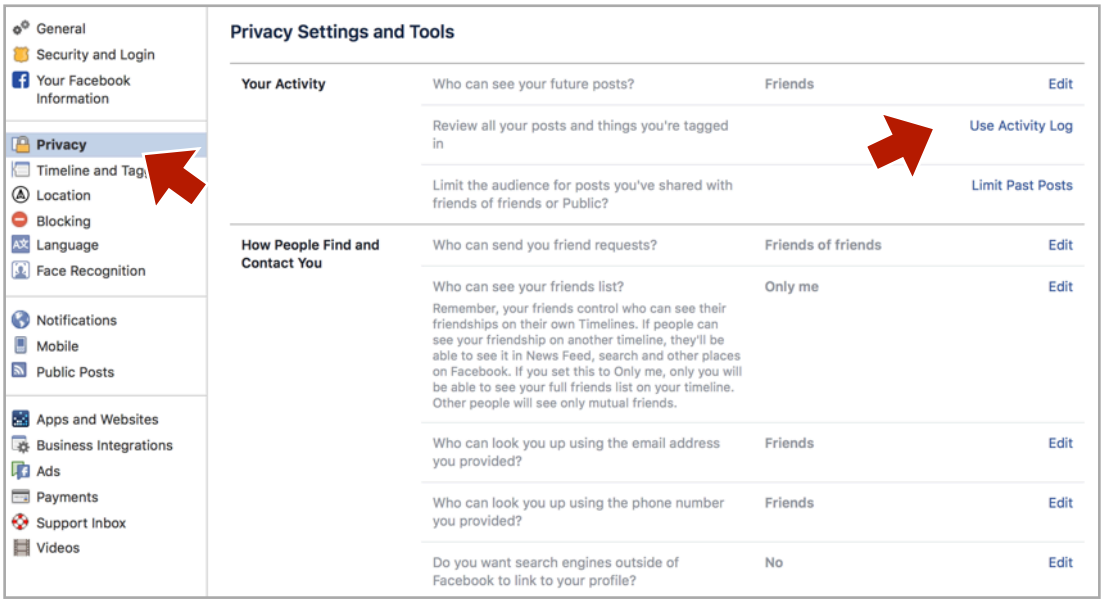


Apple Mobile F.B - click ☰ symbol lower right menu, scroll down to "Settings & Privacy" - "Settings" - "Privacy".
Android Mobile F.B - Click "More" Symbol - Scroll to "Privacy" set all as below.

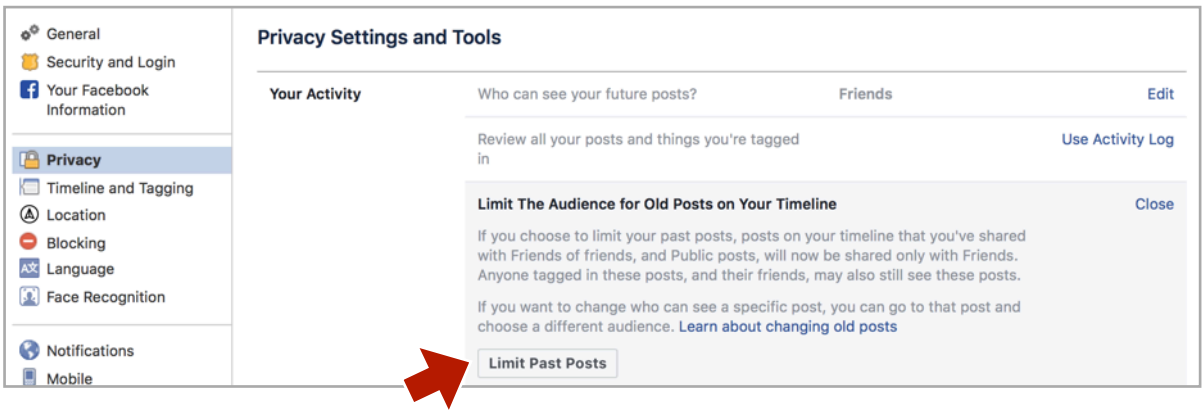
1. Go to downward arrow top right, scroll down to "Settings" on drop down menu. In next window click "Privacy" in left side menu. Set all to the most private options, as below.

Note: "Use Activity Log" is where all your posts, comments and likes are listed. You can delete your past posts one by one from there if needed. Or set all past posts back to "Friends Only"

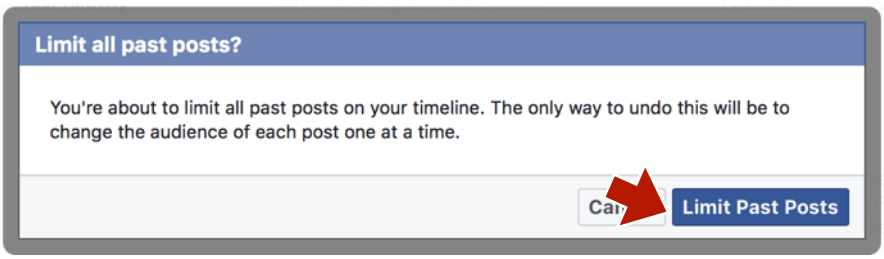
2. Set all settings as per below picture.



3. Select "Limit Old Posts". This sets all past posts back to "Friends" (not public).



4. Select "Limit Past Posts"

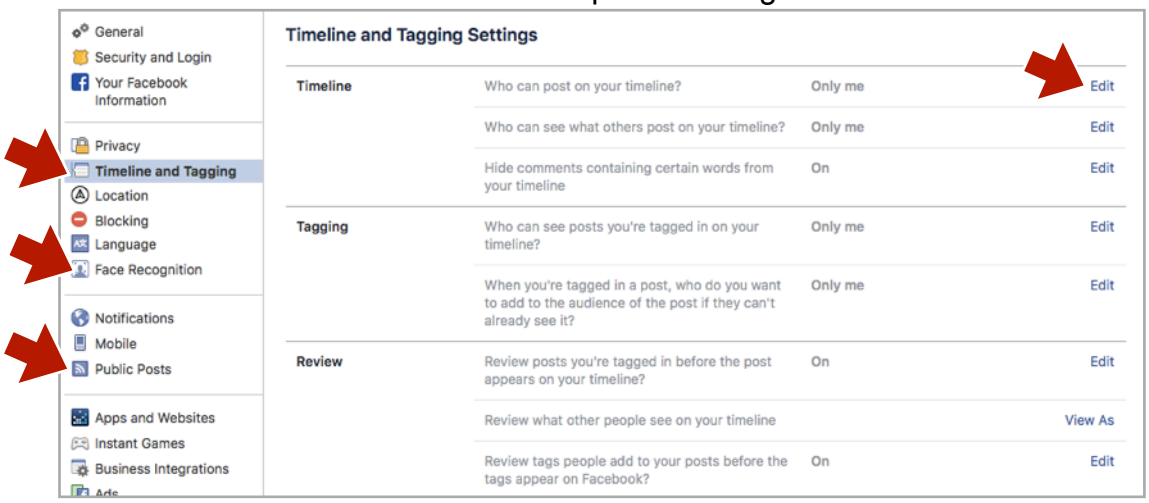


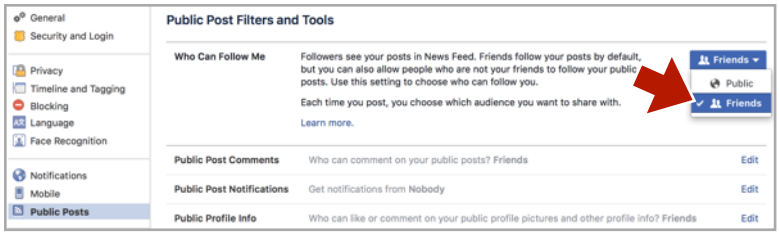
Facebook Privacy Settings

Still in “Settings” go down to “Timeline and Tagging” and set all settings to “Friends” or “Only Me” etc, as below by clicking “Edit” next to each setting.

Scroll down to Face Recognition and select your preference. Do you want Facebook to scan your face in photos?

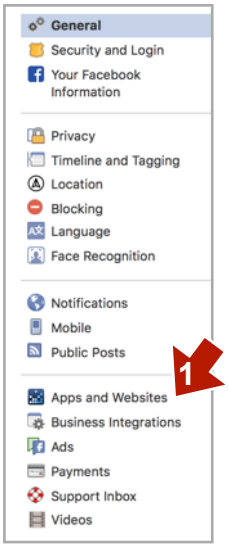
Scroll down to “Public Posts”: Set all to most private settings “Friends” not “Public”.

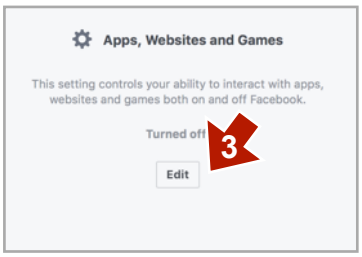


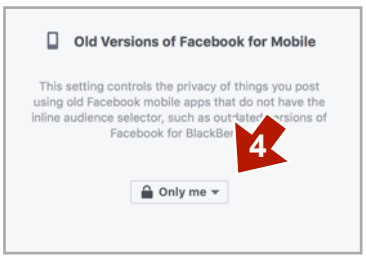


App Settings

1. Apps can share your information and preferences. Go to “Apps and Websites: Then the “Active” Tab and delete Apps you don’t use by ticking and click “Remove”. 2. Or click “View and edit” and set privacy to “Only Me”. 3. If you have removed all apps you can turn off this facility if you don’t wish to connect apps or other websites to your account by clicking “Edit” 4. Set this box “Old versions…” to “Only Me”







Mobile FB Go to “More” ☰ 1. “Settings & Privacy” - “Settings” 2. scroll to “Apps and websites” - Preferences - “Apps,websites and games” Click “Edit” next to the app and set privacy to “Only Me” or scroll down to “Remove App” 3. Turn off “Apps, websites” facility if not needed On previous page 4. Set “Games and app notifications to “No” 5. “Old versions of Facebook” set to “Only Me” Exit back out to save settings.

Blocking Abuse On Facebook P.C or Laptop

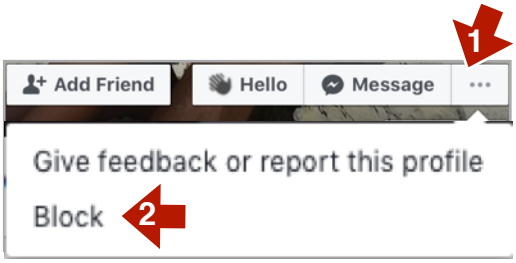
Mobile FB click “More” ☰ lower right menu - scroll right down to “Settings & Privacy” “Settings” scroll down to blocking

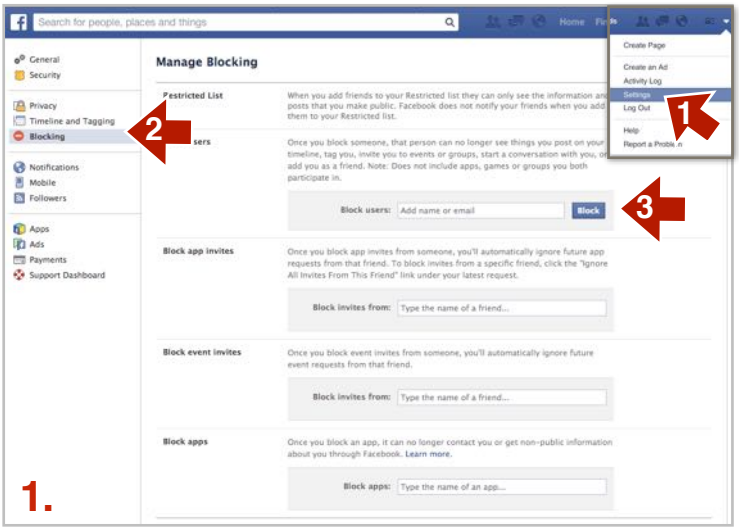
1. Blocking Apps And Users

1. Go to Facebook “Settings”
2. “Blocking”
3. “Block users” enter details.

Block messages, apps etc here.

2. You can also block users by going to their profile and blocking them from the (…) Menu. (as below).

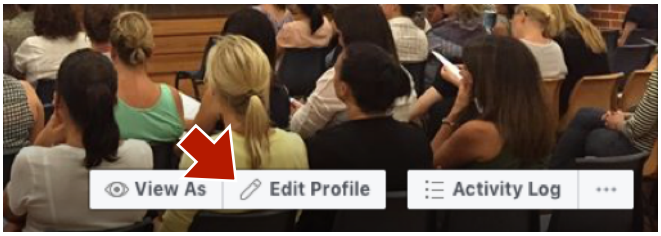




3. Hide and report comments by clicking the … menu top right of the comment. Then select “Hide Comment” or “Delete comment and block user”.

Hide Your Personal Information on Facebook

To protect all your private information from scammers and bullies select “Edit Profile” from your profile page, scroll down to “Edit Your About Info” and set all your info in every section to “Only Me” or “Friends” by clicking “Options” - “Edit” and then change the visibility. (P.C or Laptop Settings)

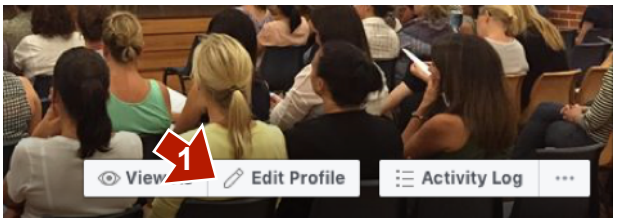


Mobile FB go to your profile page by clicking your profile pic. Click “Edit Profile” icon top right. Then Scroll down to “Edit your About Info” Click the edit icon for each section and one by one, set all to “Only Me” or “Friends”. Hide birthdate or change.

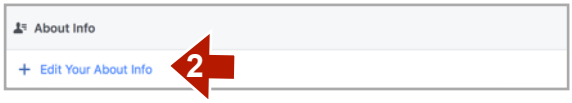
Hide Birthdate On Facebook P.C or Laptop

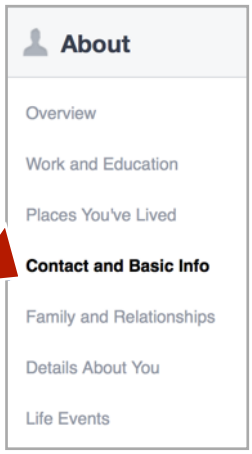
Hiding your birth date is important for security and to protect against identity theft. You can leave the day of your birthday visible to friends so that you get “Happy Birthday” wishes, but it is best to set the year of birth to “Only Me” for extra security.

1. Go To Your Profile Page, then to "Edit Profile" bottom right of your “Cover Picture”



2. Scroll down the bottom of pop up menu, click “Edit Your About Info”





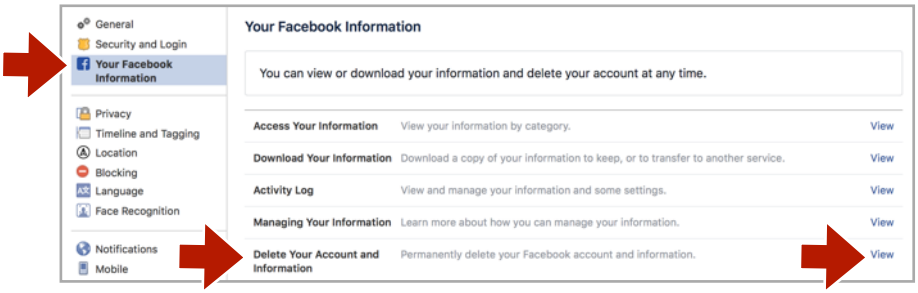
3. Scroll down to “Contact and Basic Info”

4. Hover cursor over “Edit” on the far right of “Basic Information” Birthday settings, click to edit.

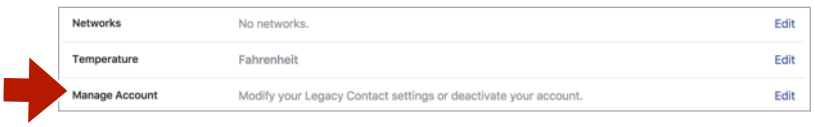
5. Set to “Friends” or “Only Me” 6. Birth year to “Only Me”.

How To Delete or Deactivate Your Facebook Account

You can either “Deactivate” your Facebook account temporarily, or you can delete your existing Facebook account permanently with all your content deleted after 30 days.
To delete permanently go to your Facebook settings - “Your Facebook Information” scroll down to Delete Your Account and Information. Click “View” and follow instructions.



To “Deactivate” or suspend your account temporarily, go to your Facebook settings then to “General” and go down to “Manage Account” and scroll to “Deactivate your account” linked text.



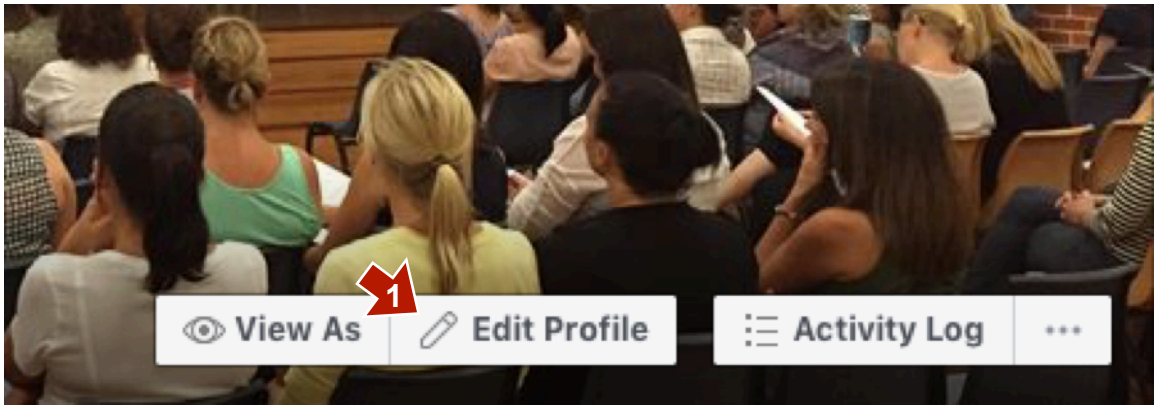
(On Mobile - click ☰ - Scroll to “Settings & Privacy/Settings/Personal Information/Manage account/Tap Deactivate, follow instructions. To delete, “Settings & Privacy/Settings”, scroll to “Your Facebook Information” then “Delete your account & information”.)

Hide Phone Number & Email On Facebook

PC Laptop Browser Settings

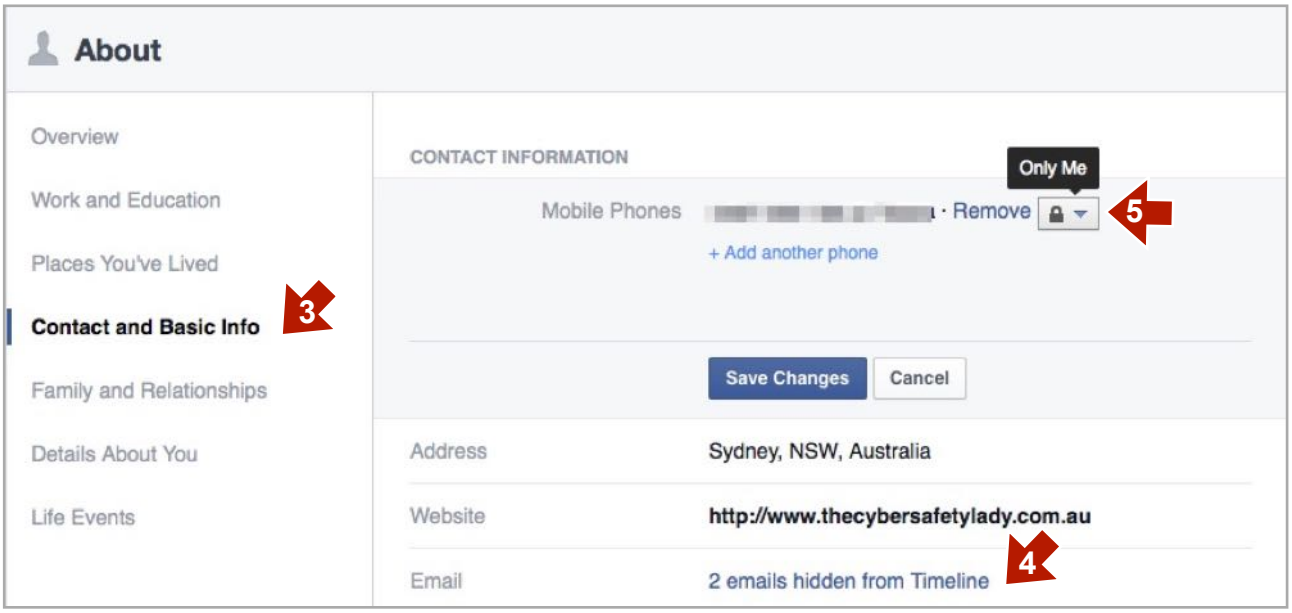
Hiding your phone number and email on Facebook can prevent spam and scams being sent to your email, phone and Facebook Messenger. A lot of cyber crime and scams are being spread through email and phone numbers. Avoid putting either online anywhere.

1. First go to your Facebook Profile and Click “Edit Profile” bottom of your “Cover Picture”



2. Scroll down the bottom of pop up menu, click “Edit Your About Info”

3. On next page click “Contact and Basic Info” in the left column.
4. Then scroll down to Email click “Edit” (far right of panel) set to “Only Me”.
5. Scroll to “Mobile Phones” and remove the number or set to "Only Me”.

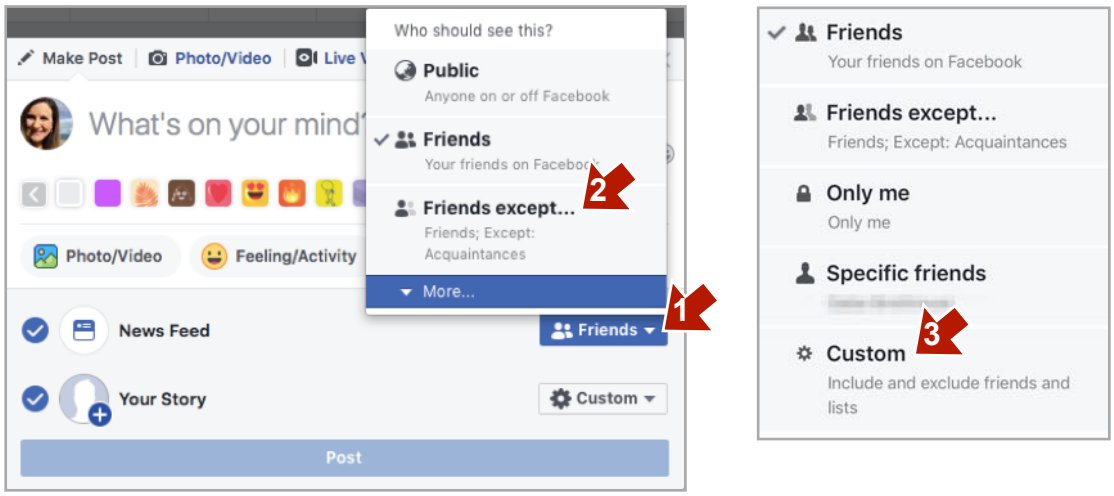


Note: It is good security to hide as much as you can in this panel.

How To Post With More Privacy On Facebook

1. Before you post an update choose who you want to post to from the drop down menu bottom right. If you choose "Public" it means the post can be seen by everyone including to people who are NOT your friends. 2. “Friends except Acquaintances” means close friends only. Go to your friends list and set your friends to either “Close Friends” or Acquaintances or leave as “friends” this helps decide what they see, and how much you see of their posts. Exclude or include friends in 3. Custom tab.

Note: If you do want to post publicly remember to change it back to “Friends” later if needed, your future posts will default to public until you do!

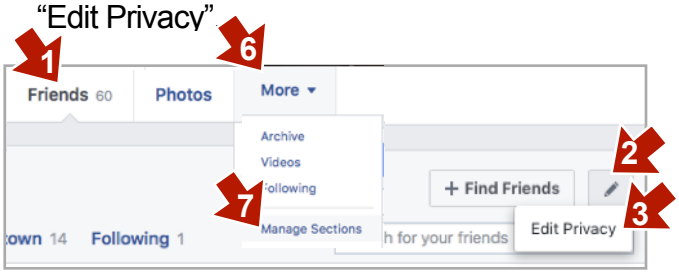


Hide Your Friends List On Facebook

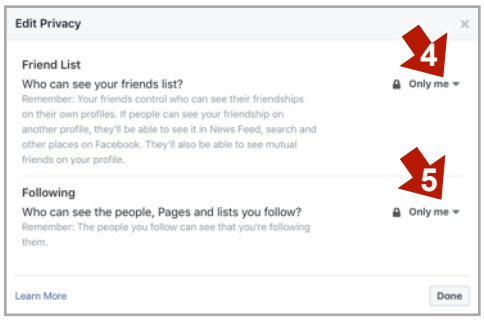
P.C - laptop only **Top Tip!** See step by step video here or scan code

Keeping your friends list private is more secure than leaving it public. Scammers, blackmailers or cyber bullies can use your friends list to spread scams or cyber bullying messages about you. Hide your friends list through Settings/Privacy “How people find and contact you” - “Who can see your friends list?” Set to “Only Me” Or as below - Note: for Mobile F.B app go to ”Settings & Privacy” “Settings” “Privacy Settings” scroll down to “Who can see your friends list” set to “Only Me”

1. Go to your profile, then to the "Friends" tab below your cover pic. 2. Click the pencil icon next to “Find Friends” & then click 3. “Edit Privacy”



4. Then select “Only Me” or “Friends” For the “Friend List” and 5. “Only Me” for “Following” options.

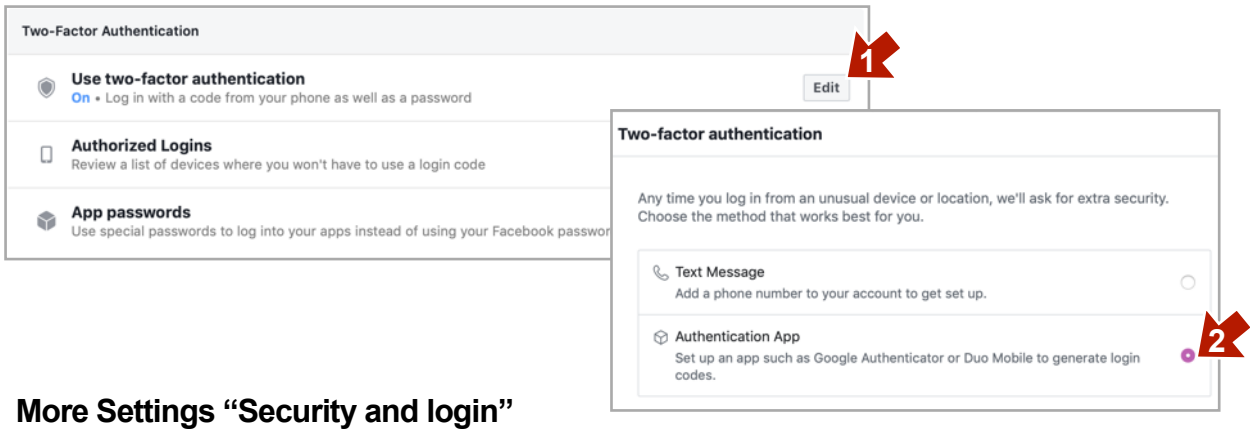


Hide Your Groups And Personal Preferences: Scammers and stalkers can use your private information, likes, and preferences to steal your identity or market scams to you. (See pic above left) Clicking 6. “More” & 7. “Manage Sections” displays a list of information that can be displayed publicly on your profile. Un-tick all of them to hide your groups, preferences and likes. The greyed out ticked options on the list cannot be un-ticked. Untick “questions” and it will disappear from the menu. (Can’t be set via a mobile device. Open settings on a P.C or Laptop)

Facebook Security Settings P.C or Laptop

Don't get your Facebook Profile Hacked! Set extra security by going to Facebooks Security settings and setting Two Factor Authentication so that you will be sent a notification through an Authenticator app like Google Authenticator or Sophos Authenticator, if someone is trying to hack into your account. Don't use SMS or your phone number unless you have to, keep your phone number off Facebook. Download an Authenticator app first on your mobile, then come back to set up, and follow the instructions on the screen.

Go to Settings/Security and Login - "Two Factor Authentication" click "Edit" and set up.



More Settings "Security and login"

Be sure you have a good strong password on your Facebook account and store it safely. 9 Letters or more, random letters symbols and numbers or use unrelated words and numbers.

Choose 3 to 5 trusted friends who can help you get your account back if the hacker has changed your password and logged you out. Be sure they really are TRUSTWORTHY!

Future Proof Your Digital Footprint!

Don't leave your personal content up online.

If you are sharing personal family photos or videos on social media or a social photo hosting site, consider deleting or archiving some past personal posts after sharing them. Keeping past posts, personal videos and photos on any social media site, may not be secure. You risk public exposure if your account is ever hacked, or if your content is shared beyond your original wishes. Be sure to use good safe passwords (8 characters/ digits or more of unrelated phrase or wording) and Two Factor verification where ever possible to prevent hacking of your accounts or cloud storage.

Your Digital Footprint

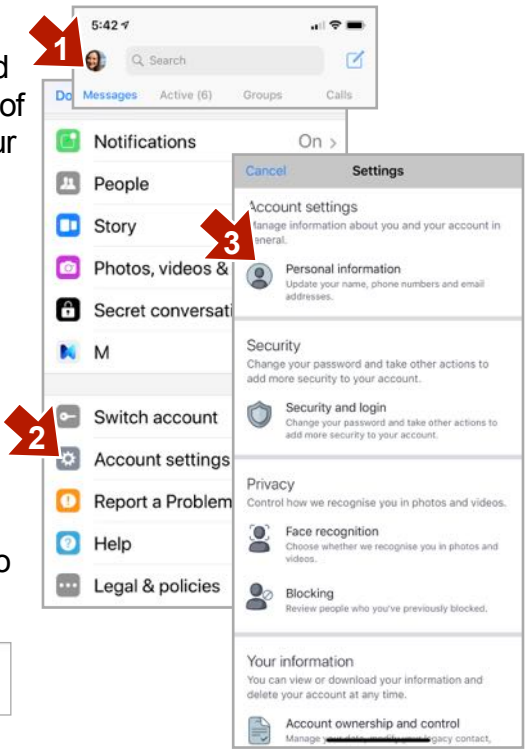
Parents: Your children may one day have a role in their community or a career that demands privacy. If you are then asked by your child to delete all the personal content that you have shared online about them, it will be more difficult to do so years down the track. Of course you cannot guarantee that copies of the posts have not already been shared. Archiving or deleting as you go certainly minimises later risk, and makes it easier to protect your child's online footprint.

To archive past Facebook posts go to the "View Activity Log" menu located under your profile cover pic and delete each post one by one. For Instagram delete posts one by one from your account. Or select photo and then click … Menu and select "Archive" or "Delete".

Facebook Messenger - Mobile

Privacy Settings

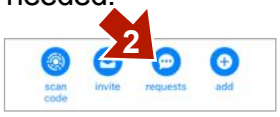
All your privacy settings for Messenger must be managed through your normal Facebook profile. To manage some of the settings on Messenger, Open Messenger 1. Click your profile Pic 2. Scroll down to “Account Settings” Click and adjust settings for your preferences.



Filtering Message Contacts

You can no longer filter who contacts you on Facebook Messenger. Anyone who has Facebook Messenger can now contact you on your Facebook Messenger app by sending a Facebook Message request.

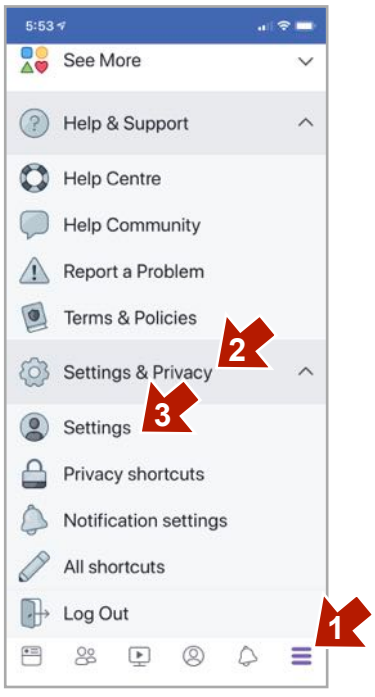
Non friends messages will show up in the “Request” tab. Open Messenger - Go to 1. “People” then 2.“Requests” to review invitations. Block or accept as needed.

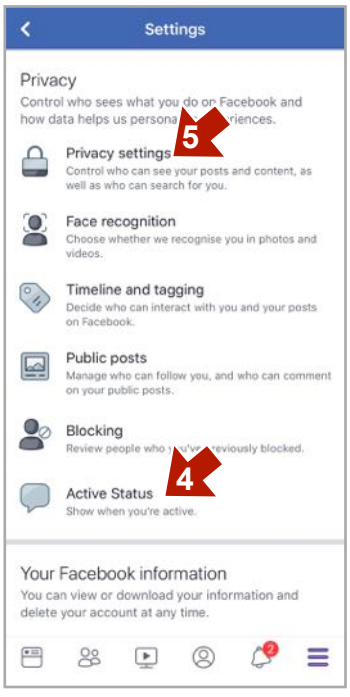


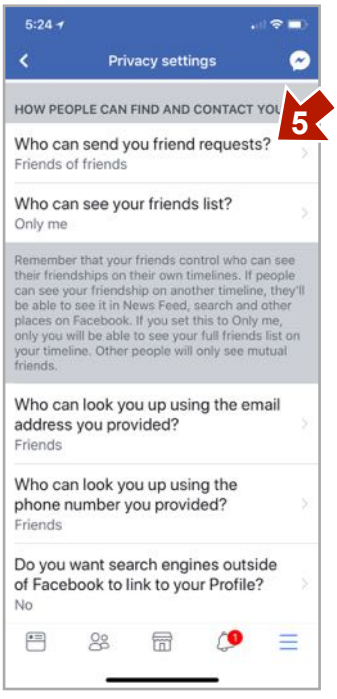
Make sure you have all your Facebook privacy settings secure by also following the “Facebook Privacy and Hiding your Private Information” instructions in this manual.

When A Stranger Calls!

Some users are reporting that they are getting random messages from strangers on Facebook Messenger. You can’t set FB Messenger to only receive “Friend” messages, but you can reduce the likelihood of getting strangers messaging you by setting up strict privacy settings the Facebook mobile app via 1.“Menu” 2.Scroll down to“Settings & Privacy” 3“Settings” 4.Turn off Active Status. 5.”Privacy settings” Set all as below.







Facebook Messenger - Blocking - Muting

You can block a contact directly through Facebook Messenger and you can “Mute” a conversation if you no longer want notifications from that chat.

To Mute

1. Go to your Messager “Home” messages list (house “Home” icon).
2. Tap and hold the message you want, select “Mute” from the pop up menu.
3. “Mute” forever or temporarily.

This will only Mute a past conversation NOT block someone from contacting you.

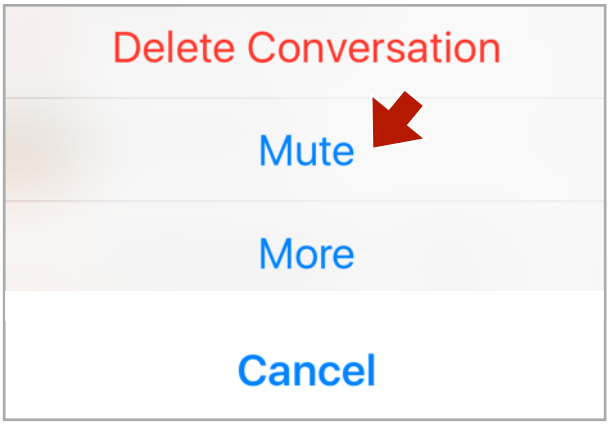
To Block A Contact

Tap and hold message from the contact you want to block in the “Home” menu - slide up. 1.Select “More” 2. Select “Block” and then slide “Block Messages” toggle to the right (Green) & click “Done” To set.

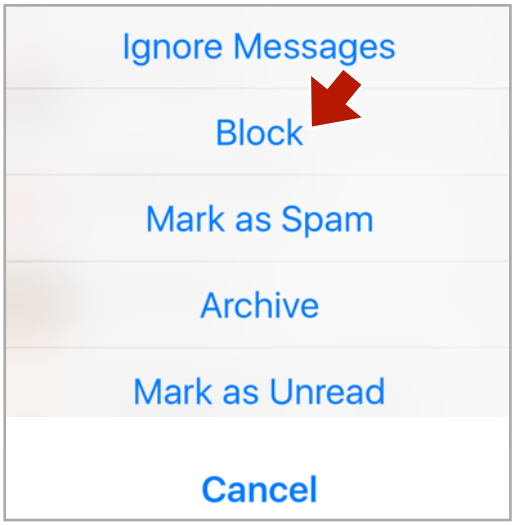
This only blocks them from messaging you. They can still be friends with you on Facebook. To block them completely also select “Block on Facebook”

You can also add them to block list in Messenger Settings. Click your profile pic to navigate to settings. Settings/People/Blocked - “Add Someone” Type in Name.

To Mute



To Block



To Delete Messages

Delete messages you don’t want, by tap and hold in “recent” “Home” view, select “Delete Conversation”.

Android Facebook Messenger Privacy: Go to “Settings” icon top right, and turn off “Synced contacts” and “location”. Scroll down to and click “Privacy” in the small print links at the bottom of settings, opens in a browser. Follow the instructions from above when in mobile Facebook privacy settings. Note: You can’t block through F.B messenger on Android use “Mark As Spam”

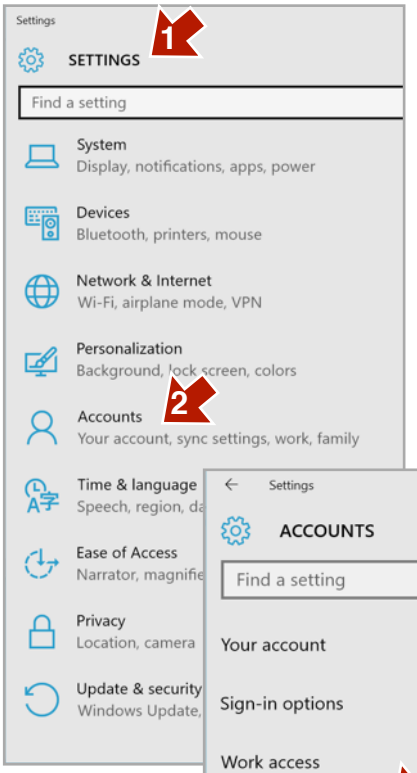
Note: This app is listed at 12+ on the iTunes store, but cannot be used without a Facebook Profile. So it is only available for children aged 13years and over, as per Facebook’s Terms Of Service age restrictions. Facebook Messenger Kids App had not been released for Australia as of publication. Oct 2018.

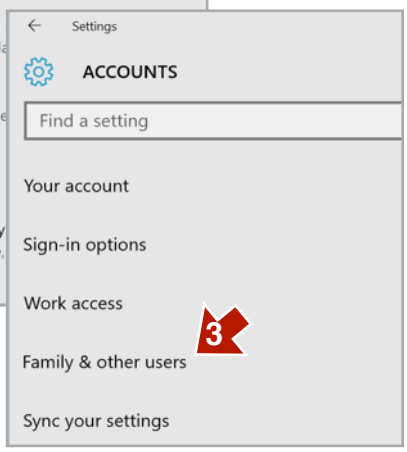
Parental Controls For Windows 10

These settings are cloud based and apply to any Windows machine your child logs into with Windows 8 or 10.

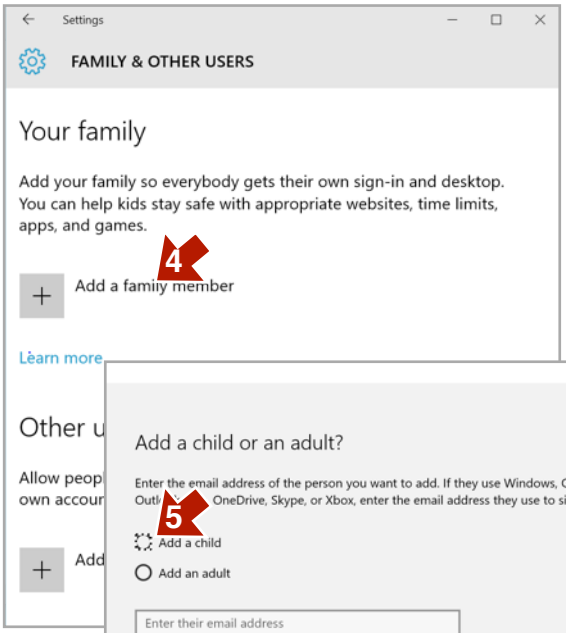
Windows sets up the account for a child depending on the age given, adult content is blocked by default. You can then manage the settings for that account online.

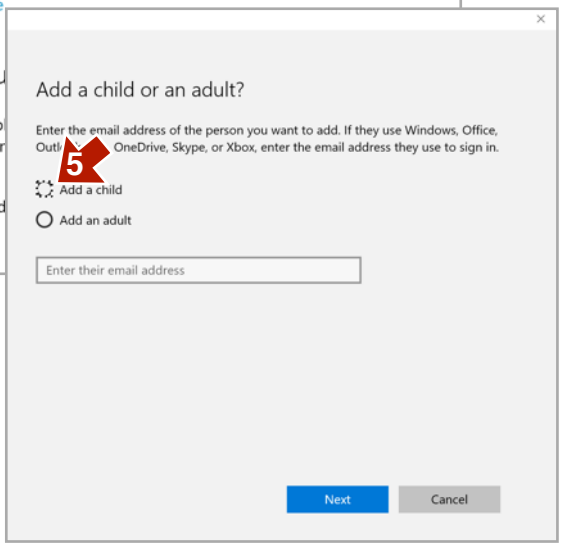
You can add blocked sites or allow them through. You can also monitor their screen time and what apps or games they play and what sites they visit.

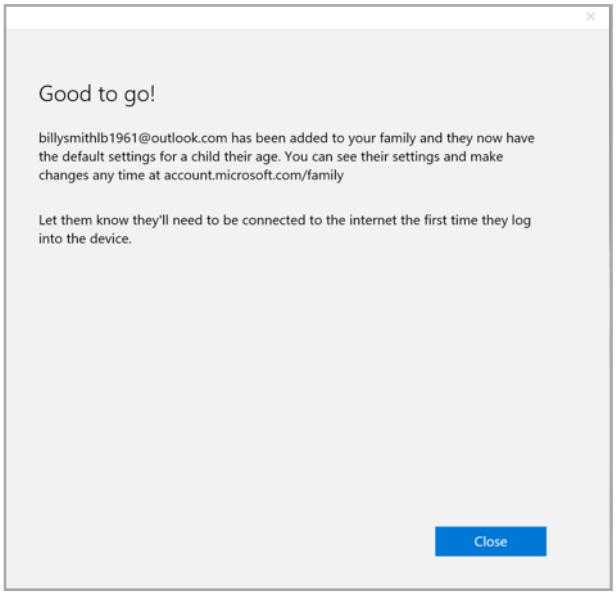




Go to 1."Settings"
2.”Accounts"
3."Family & other users"
4.”Add Family Member"
5.”Add a Child" and then follow all the prompts.





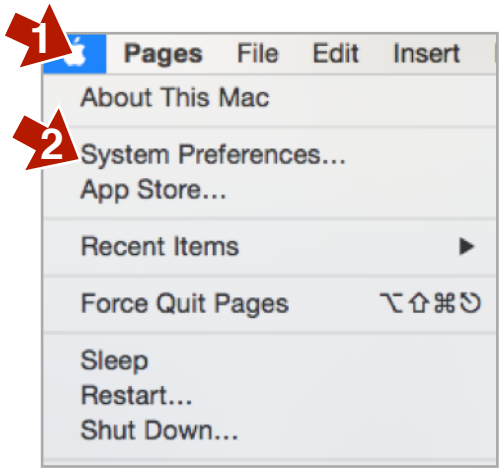


Once you have set up a parental controlled account for your child, you can then alter the controls, add websites you want to blacklist and monitor their online activity at www.account.microsoft.com.family You can log in to do this from any browser, mobile or P.C remotely.

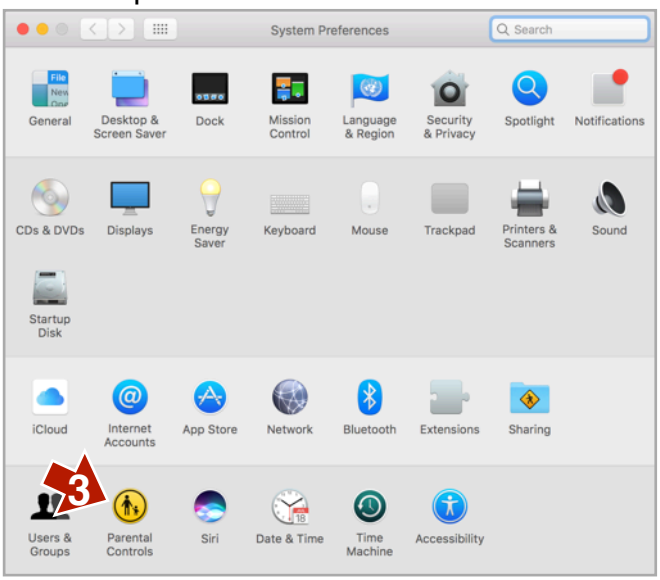
Parental Controls On A iMac or Macbook

A parental controlled account is fantastic for younger children if you prefer them to have an account with only basic access to the computer. NOTE: You must be an administrator to set up parental controlled accounts.

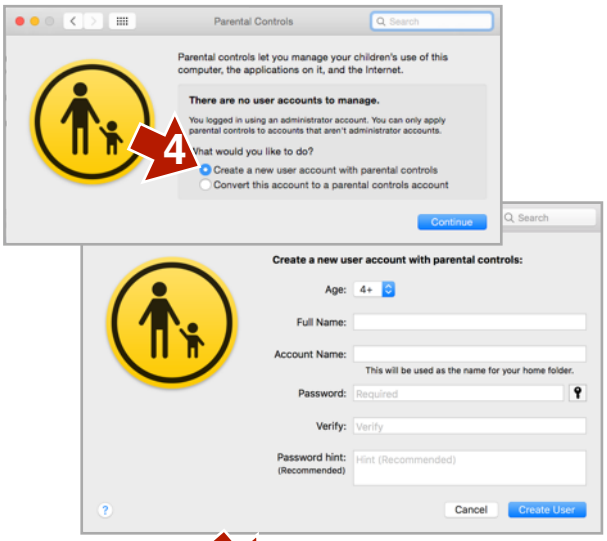
1. First go to the Apple symbol top left of your screen.
2. "System Preferences".



3. Then scroll down to “Parental Controls” In next window “Click lock icon to make changes” - input your admin password.



4. If you don't have an existing user account to modify, then create one.

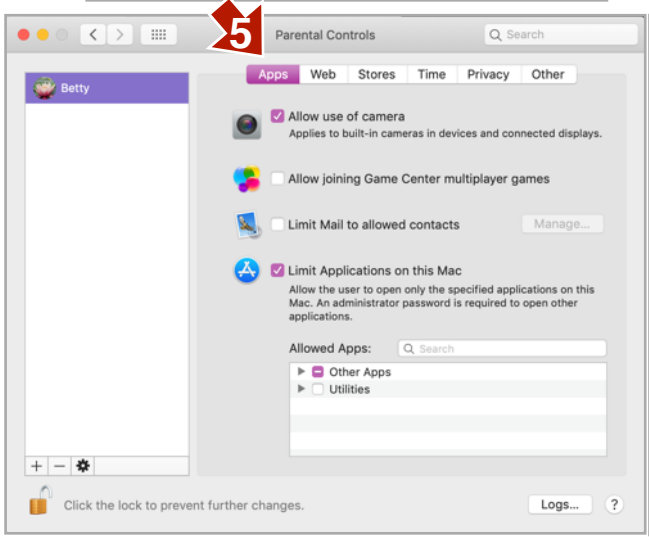


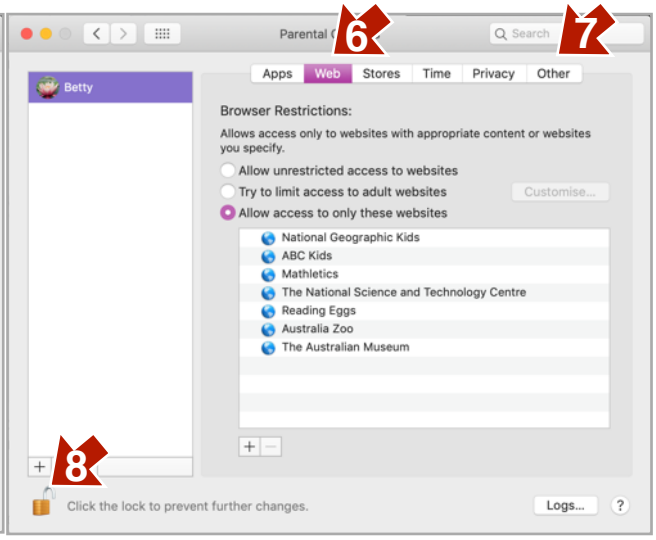
5.You can then set up the parental controlled account to restrict any applications.

6.You can also restrict which websites they visit, disable downloading apps, and set time limits and privacy.

7.The “Other” menu includes restrictions for disabling Siri, and hiding profanity in the built in Dictionary.

8.Click the “lock” to save.





NEW Apple parental controls “Screen Time”

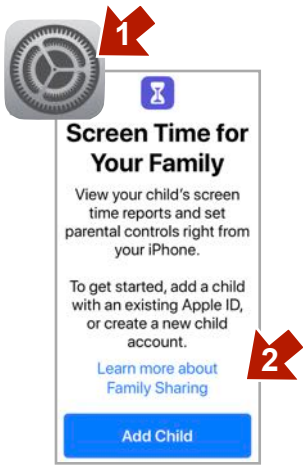
iOS12 Update

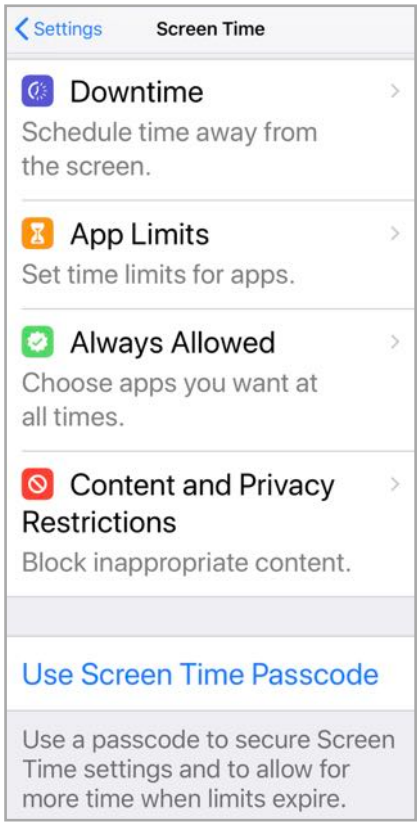
The latest software update for Apple mobile devices like iPods, iPhones and iPads is iOS12. This new operating system has a new centralised moderation and parental control system called “Screen Time” this replaces the former parental control system known as “Restrictions”.

“Screen Time” settings include all the previous parental controls and filtering you have previously enabled, but now allows you to monitor your child’s use through weekly reports, and control settings and screen time remotely. Apples Family Sharing now allows you to monitor and control a child’s use from your own device through the “Screen Time” menu.

More information on “Screen Time” Here https://support.apple.com/en-au/HT201304

If you haven’t set up your child's device on Family Sharing, you will prompted to add or create a new child account, to include in your family sharing profile when you go to “Screen Time” More on family sharing Here: https://support.apple.com/en-au/HT201060





To Enable Screen Time -

1. Go to Settings on your, or your child’s device.
2. Scroll down to “Screen Time”
3. Follow the prompts to set up a new child account or set up Screen Time on a child’s account or device.
4. Set to share across multiple devices if your child has more than one device, iPhone, iPad

In Screen Time settings you can select the settings appropriate for your child.

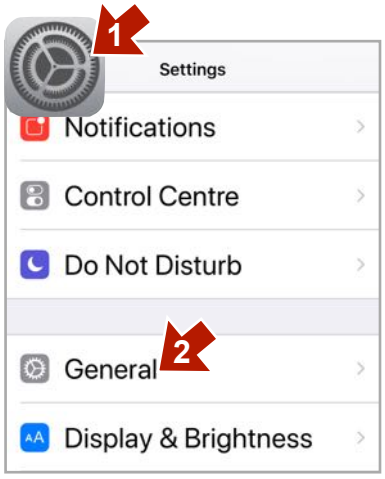
1. Set a “Downtime” schedule to disable device, 8pm - 7am for e.g or set to restrict use to only essential apps.
2. Set time limits on groups of apps, or individual apps through “App Limits”. Social media or games, one hour a day for e.g, then blocked.
3. Set “Always Allowed" for apps e.g Books, Educational apps for use at all times including during “Downtime” .
4. **“Content and Privacy Restrictions”**
   - Set age restrictions or block specific apps
   - Password block installing new apps
   - Disable In-app Purchases via iTunes & App Store Purchases
   - Block/ban Safari browser for younger children
   - Filter explicit language from books, films, music
   - Block location on apps, like social media or games
   - Block porn via “Web Content” set “Limit Adult Websites”. Or block Safari if not needed.
   - Block adding friends to block strangers
   - Password block any settings changes

Important: Set a strong passcode to prevent your child changing the settings. You will need the passcode to allow access to blocked content or to change settings.

Parental Controls Apple iPhone, iPod, iPad

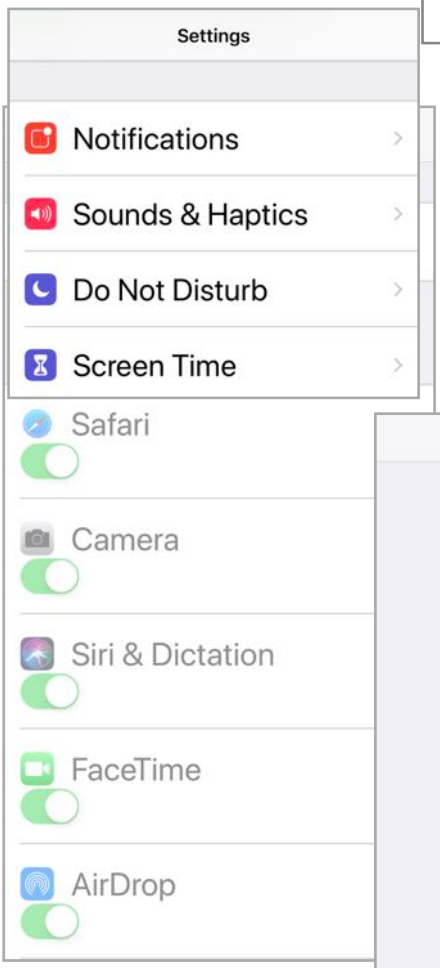
Old Operating System iOS 7 - iOS11

1. Go into “Settings” then scroll down to 2. “General”.

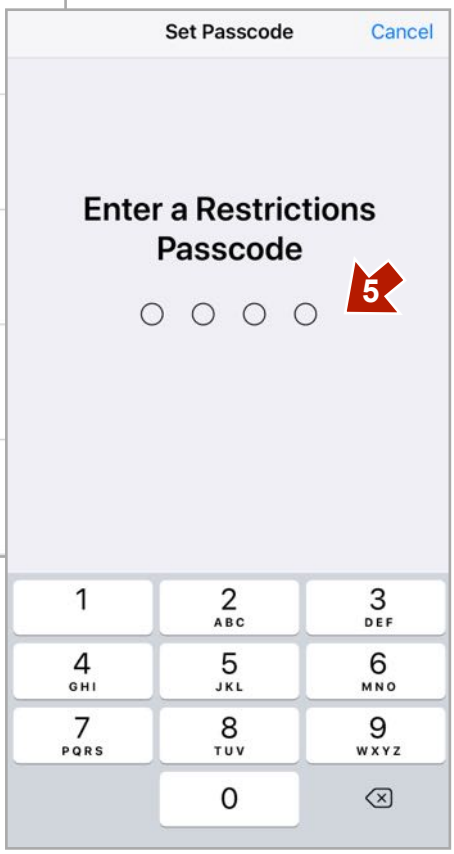


iOS12 - New settings for parental controls. Go to “Settings”, scroll down to “Screentime”. Set a Screen Time Passcode. Then set “Content & Privacy Restrictions”, “Downtime”, “App Limits”, “Always allowed” as needed. See pg 40

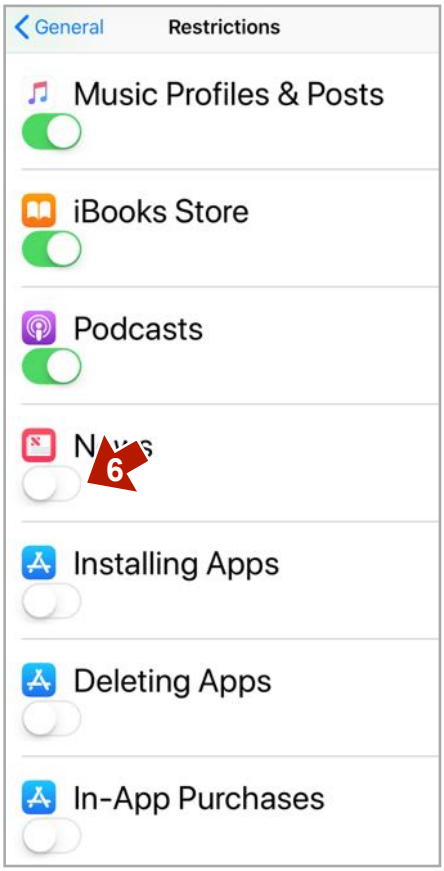
3. Scroll Down To “Restrictions” and click. Click “Enable Restrictions”



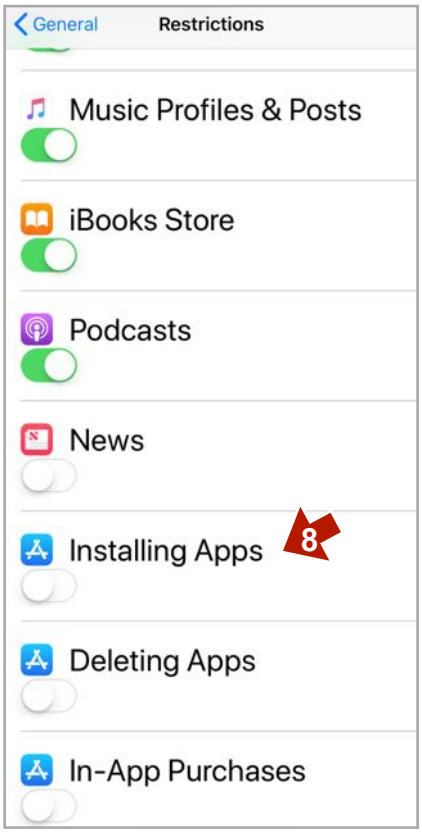
5. Set a secret Password for “Restrictions”, so that your child can’t alter them.



6. To Disable any apps slide settings to the left/white.



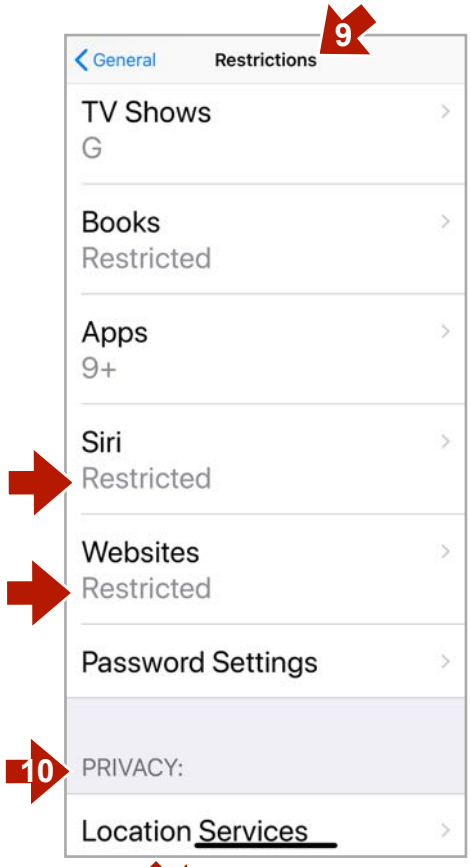
8. To prevent your child downloading apps without your permission. Scroll down “Restrictions” and disable “Installing/Deleting/In-App Purchases” (Slide setting to the left, as below). Your child now must seek your password and permission to install/delete new apps. The app store icon will be missing from the device screen.



9. Then scroll down to “Allowed Content” set each option for your child’s age group.

Websites & Siri Should Be Set To Restricted to protect agains adult content.

10. Under Privacy set each to “Don’t Allow Changes” This prevents your child from changing your restrictions to each setting.



11. Finally Scroll to bottom of the “Restrictions” page to “Game Centre” settings and select the option for disallowing “Multiplayer Games” (e.g. Clash Of Clans) and “Adding Friends” if you prefer your child not to play online games or add friends/strangers to their games. This won’t prevent chat in games. Some games you can hide chat some you cannot. You can also disallow screen recording if you wish, some children like to record video from friends or game play.

Android: Google now have “Family Link” Go to https://families.google.com/familylink/ to find out more. Some of the restrictions are -

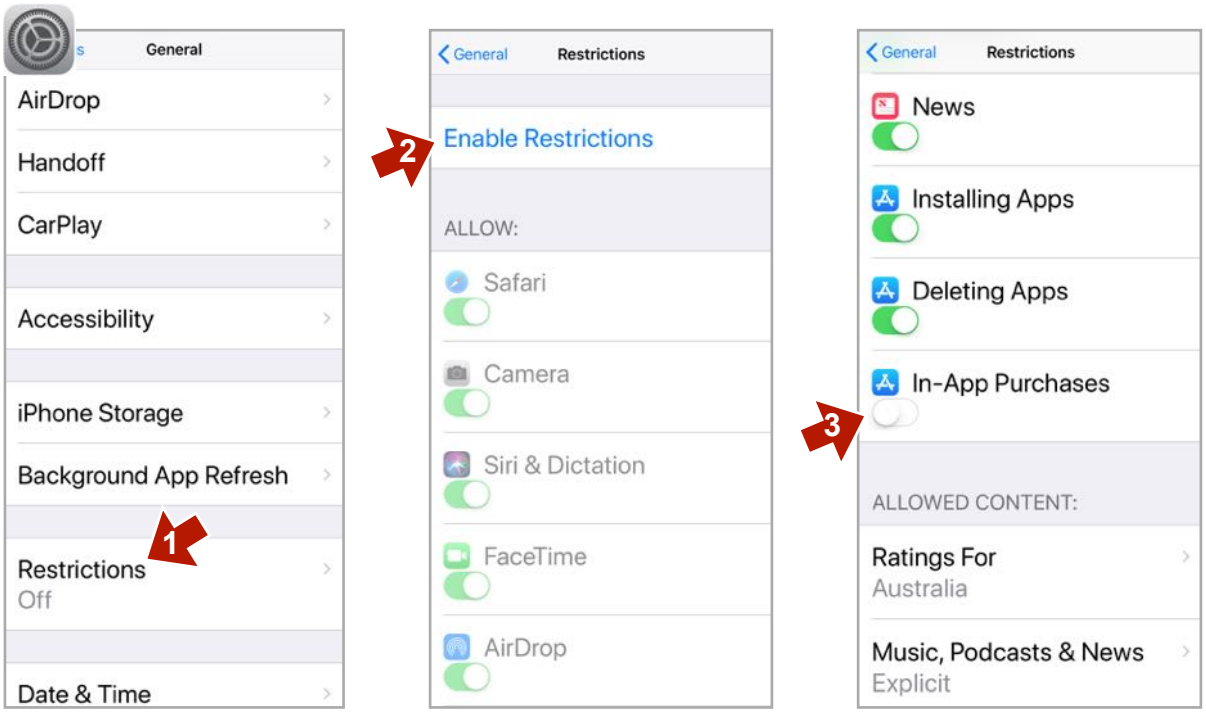
- Approve your child’s downloads & purchases from Google Play/limit visibility of content
- Manage settings such as SafeSearch for Google Search;
- Review your child’s app permissions on Android
- Set screen time limits on your child’s Android devices;
- See the location of your child’s Android device;
- Manage the activity settings for your child’s Google Account

In App Purchases Apple Mobile

Free apps often come with hidden costs. To prevent your child spending up big on their mobile games, disable the In-App Purchases in settings.

Android: Go to Google Play store to disable through the devices ≡ "settings" and disable In-App Purchases. Exit out of settings to save.

Apple: Go to "Settings" then 1."General" scroll down to 2."Enable Restrictions" Click & set a secret 4 digit password 3.Scroll down to "In-App Purchases" and toggle/swipe setting button to left to turn off, as seen below. Set any other restrictions appropriate then, exit back out of all menus to save settings.



AN IMPORTANT NOTE: As with all devices that can potentially connect to the internet you must supervise your child's use of the device. There are no fail-safe safety settings or parental controls.

Note: Age ratings on iTunes & Google+ are unreliable. Some apps that should be rated 13+ are rated 12+ like Facebook and Instagram. Make sure your child always asks permission for new apps.

New Parental Controls and Family Sharing on iTunes. You can share an iTunes accounts with up to six family members so that you can better supervise your children's purchases and messaging, see below to set up. In the latest Apple Mobile Update iOS12 there are more parental controls like time restrictions and statistics to see how much time your child is spending on various apps. This will work through Family Sharing, so make sure you have it set up. See pg 40

On Mac go to the "Apple" menu - "System Preferences" - "iCloud" - "Manage Family" and click the Add button (+).

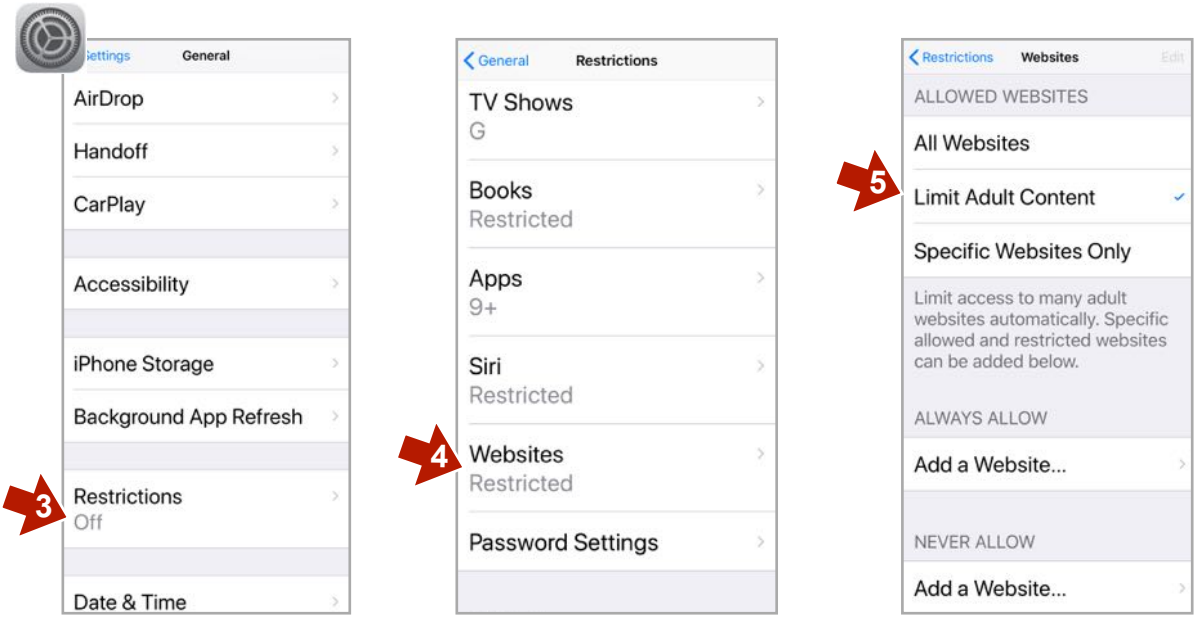
On Mobile Go to "Settings" - click "Your Name (Apple ID, iCloud ect…)" - "Family Sharing" and tap "Get Started" or "Create an Apple ID for a child." or "Add Family Member"

For Young Drivers: You can now set your phone to automatically go silent when you are driving. Go to Settings/Do Not Disturb/Do Not Disturb While Driving and Activate/Automatically

Browser Safe Search - Apple Mobile -iOS11

These settings help prevent your child accessing adult content whilst using any browser on Apple mobile devices including iPhones, iPods, iPads. Note: Set other restrictions for blocking adult content also in restrictions. For the new iOS12 system go to Screentime/content and privacy restrictions/content restrictions/Web Content/Limit Adult Websites and exit out.

1. Go to Settings 2. Scroll down to “General” 3. Click on “Restrictions” and set a password if you haven’t already 4. Click on “Websites” 5 Select either “Limit Adult Content” or “Specific Websites Only” to only allow certain websites.

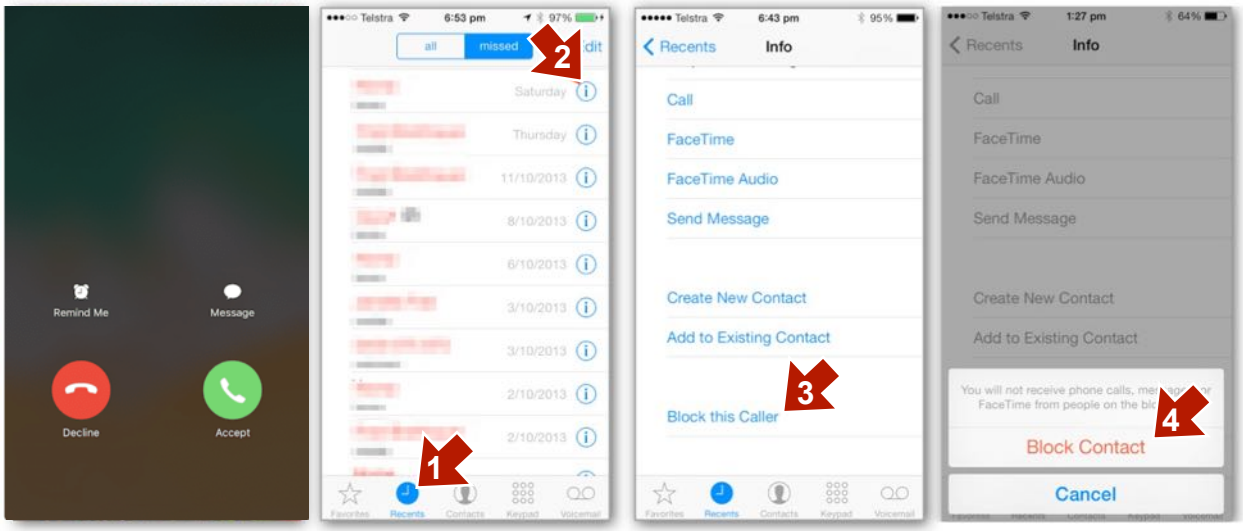


Call Message & Text Blocking On Apple Mobile

Note: You cannot block any calls from "Blocked" or "No Caller ID" calls.

How To Block:
Decline the incoming call. Then tap the “Phone” icon & your 1.“Recents” calls list, select the 2. “i” for information icon, scroll down to the very bottom of the page and select 3. “Block this Caller” Then 4. “Block Contact”. Do the same for messages or texts.

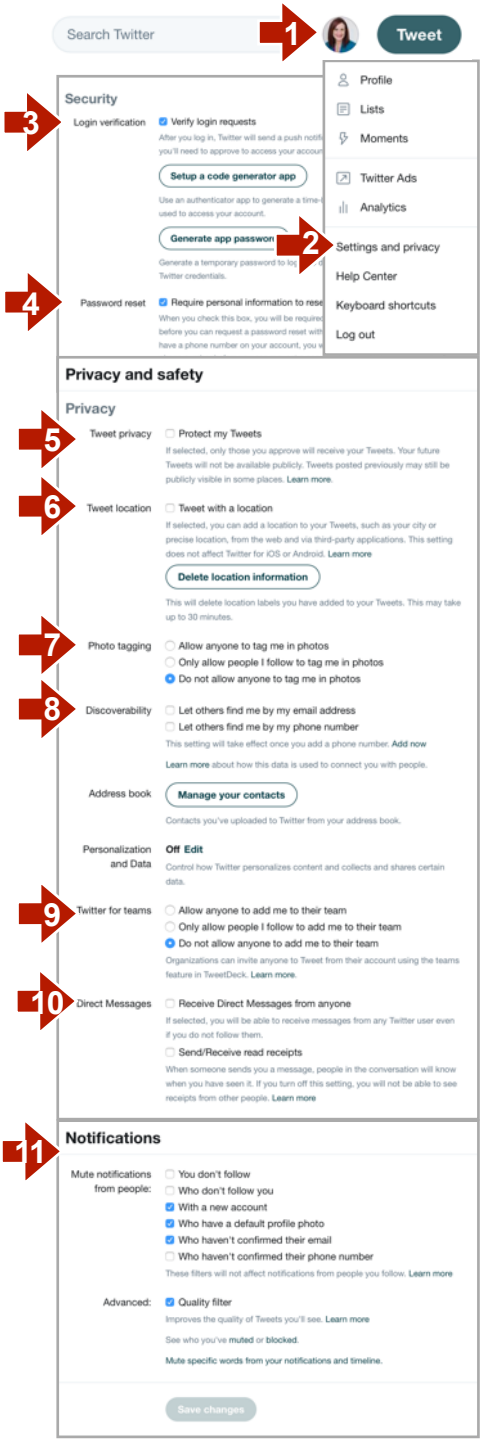
Android: Open the Phone app. Tap the 3-dot icon (top-right corner). Select “Call Settings.” Select “Reject Calls.” Tap the “+” button and add the numbers you want blocked.



Ignore Phone Call | Click on Recents - i | Scroll to bottom of screen | Click “Block Contact”

Security Settings For Twitter PC or Laptop Browser

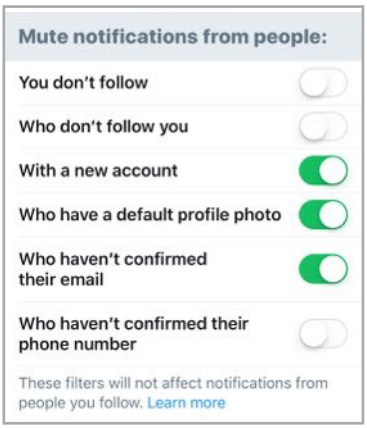
1. Log into Twitter - click your profile picture to bring up settings menu.
2. Scroll down click “Settings & Privacy”.
3. Scroll down the “Account” menu and set up “Verify login requests” under “Security”. This will then send a code to your phone or Authentication app, when logging in from a new browser or device. Protects account from hackers.
4. Password Reset: Tick “Require personal information” to reset your password.
5. Go to Privacy & Safety in left column: Select “Protect My Tweets” to approve all followers, your Tweets will then be private, shown to followers only. **Note:** All tweets can be screen captured & shared.
6. Tweet Location: Un-tick “Tweet with a location” and “Delete all location information” for extra privacy.
7. Set “Photo Tagging” to “Do not allow anyone to tag me in photos”.
8. Un-tick both settings in “Discoverability” to prevent others with your email or phone number finding you on Twitter. Don’t sync address book with Twitter
9. Twitter For Teams: Disable unless you want to share a Twitter account.
10. Untick “Receive Direct Messages From Anyone”
11. Safety: “Hide sensitive Content” and “Remove blocked and muted accounts” Also click on “Notifications” side menu. Note: New unverified accounts without a profile pic can be used for spam and trolling. Set as needed and tick quality filter.



Twitter Mobile App

Open mobile Twitter.

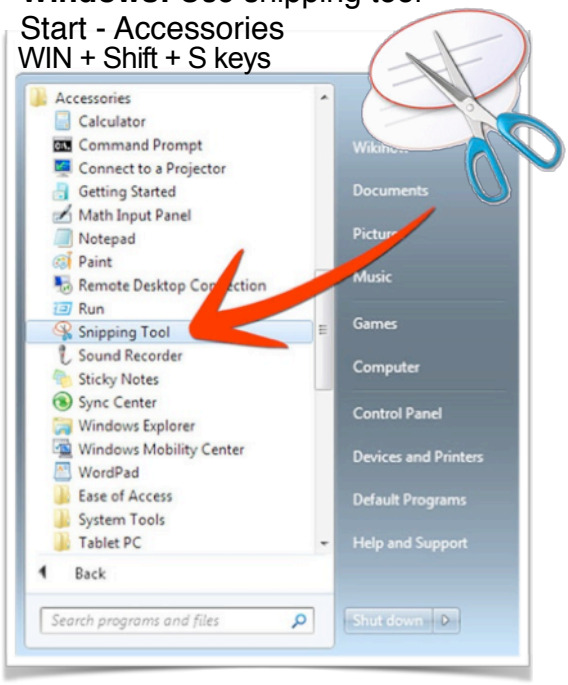
1. Click on your profile pic.
2. Click “Settings and Privacy”
3. Click “Privacy and Safety” where you can protect your tweets, prevent direct messaging and through “Discoverability filter how others find you on Twitter. Don’t sync address book.
4. Scroll down and click “Notifications” Where you can set a Quality filter and also click “Advanced Filters” to Mute notifications from new or unverified accounts if you have a problem with trolls.
5. Disable precise location for safety and privacy.



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.

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.

Should Kids Under 13 Years of Age Be On Social Media?

Some 7.5 million of the 20 million minors who used Facebook in the past year were younger than 13, and a million of them were bullied, harassed or threatened on the site, says a study released Tuesday.

Even more troubling, more than five million Facebook users were 10 years old or younger, and they were allowed to use Facebook largely without parental supervision leaving them vulnerable to threats ranging from malware to sexual predators, the State of the Net survey by Consumer Reports found." From a 2011 article on Dawn.com

Facebook's and Instagrams terms of service stipulate that users must be over 13 years of age to use Facebook, even though both are rated 12+ on iTunes. Online age restrictions are set by COPPA "Children's Online Privacy Protection Act" to protect children's privacy and their well being. When you first create an account on Facebook you have to enter your date of birth, but If you are under 13 years of age, in order to sign up you have to lie about your age. If Facebook find out, through reporting or otherwise, that a Facebook account is being used by an under 13yr old they may forcibly remove it. But according to the above figures, an enormous number of children's accounts are going unreported. It is clearly too easy for children underage to create accounts.

There are very real risks for younger children who use social media like Snapchat, Instagram and Facebook. Risks such as "stranger danger", bullying, unsupervised messaging and exposure to adult content. If your child makes an embarrassing or unwise post, the post may be easily copied/screen shot and shared on, and then potentially thousands could view it.

Unfortunately supervising or "Friending" your child on social media won't protect them from being hurt. Your child is only as safe as their friends allow them to be. If your child's friends aren't supervised, if their friends are immature and cruel, your child might be at risk. Any innocent post can be ridiculed and passed on to the point that it may go viral, and deleting the post and comments permanently might be impossible. Younger children and their friends need to be ready for the responsibility and the permanence of adult online platforms.

How Cyber Savvy Are You?

If you know your child wants a social media profile and they are under 13 years of age, ask yourself seriously if you have the ability to supervise them AND their friends? Do you know how to set all the privacy/security settings? Do you want to keep up to date on all the privacy changes? Are you prepared to have an account yourself and "Friend" your own child?

Do you understand how to avert bullying online, and how best to respond? Can you be sure that your child will not have one of their posts ridiculed and passed on to possibly thousands of people? Are your child's friends parents cyber savvy?

If you can't answer positively to all these questions, it would be wise to delay your child's participation on public social media. Not every parent has the time to monitor their child effectively online and if you can't monitor your child on Facebook for 100% of the time when they are underage, you and your child may well be very sorry. For older Teens, the same as above needs to apply, but older teens are less vulnerable and hopefully more mature. **Note:** If YOU can't teach your children safe online behaviour, find someone who can.

Privacy Settings:

Most adults I speak to *think* they understand social media apps, with secure privacy settings enabled, but sadly most don't. This manual shows you how to use the "View As" menu to test your own Facebook privacy settings. Test your profile first to find out what you are showing publicly, and then test your child's, you might be dismayed at how much personal information you are sharing with the world.

Privacy settings are essential for all users who want to keep their account visible only to friends. If you do allow your younger child to have a social media profile, how certain are you that you know what settings to enable or disable to help protect your child?

More and more social media accounts are being reviewed by companies and organisations to assess suitability and gain insight into character. Your child doesn't need their future college, employer, banking institute, or landlord to be able to click back and see posts that they uploaded at ten years old, if they inadvertently posted something embarrassing publicly.

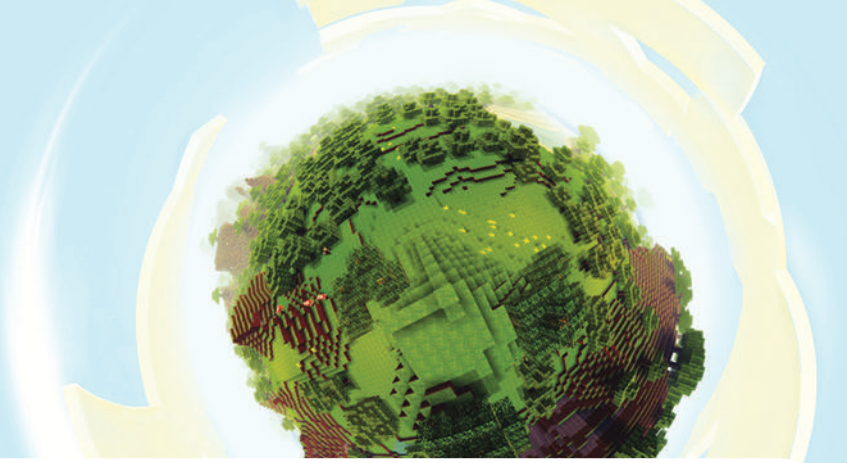
Bullying With Fake Accounts:

Impersonation of Facebook, Snapchat and Instagram accounts is growing at an alarming rate. If someone sets up a fake account in your child's name to bully them, it can be very damaging. Applying to have the fake account removed can sometimes be a long painful process, and in the mean time the nasty posts seeming to have come from your child might have been copied and passed on further than their friends. The younger the child, the harder it may be to recover from such an attack. Mature resilience and online street smarts is required to survive the adult online social media world.

Predators On Facebook:

Some adults and older children may use Facebook to groom younger users for online sex, sexual photos and video, by pretending to be a friend or another child or a celebrity. Your child needs to be able to resist a cunning predator that pretends to care about them. Some pedophiles use voice changers on voice messaging apps like Skype or Facebook Messenger to con both parents and children into believing they are genuine children. Predators may copy real social media profiles of other children to groom and guide children into trusting them before requesting, sometimes with threats, for inappropriate photos of your child. If a pedophile manages to solicit a nude photo from your child, it may be impossible to retrieve it, or trace the perpetrator.

Finally: Your child is only as safe as their friends allow them to be on social media. No amount of supervision can prevent a post from your child going "viral" if someone shares it with a bad comment or changes the content. Are you sure your child and your child's friends old enough to handle the responsibility of the adult public online world?



Published 28th May 2011

Parents Guide To Minecraft

Guest Post By Will.B

What is Minecraft?

Minecraft is a virtual 3D Lego-like building game for the computer, where the player is free to make anything they want. It is a great way to encourage creativity and helps to build on team skills and working together to reach personal goals.

Is Minecraft safe for kids?

Certainly, if it is used correctly and if you are restricting whom your child is playing with. However, there are many public servers for Minecraft that allow players to talk to complete strangers through a chat. Minecraft does not have any graphic content, but there are monsters such as spiders and zombies. However, the monsters in Minecraft are very cartoon-like. It is rated 8+

The Different Versions of Minecraft

- The PC version is by far the most used and provides a large variety of user-made servers (A place where many people from different places can play together) to play on, meaning that the likelihood of you meeting a complete stranger online is almost certain. However, if you do not wish for your child to be playing on a public server with strangers, they may create their own server and only the people they invite will be allowed on it. (Experts and advanced users only) Go to the Minecraft Wikki for instructions. Search for “Setting up a server”. Minecraft Realms is a paid subscription to a version of Minecraft where you can also set up your own private server easily.

- Minecraft Pocket Edition is available for iOS Apple and Android devices, and has a smaller community, but still allows players to play and communicate with one another. There is a huge reduction in the risk associated with this version of the game, but there are fewer features than the PC version.

- The console version of Minecraft is available for Xbox and PlayStation, and is pretty popular, but still has a high risk of meeting a complete stranger. However, making a private server where only your child’s friends can play on it is very easy.

Privacy Settings On Minecraft:

Currently in Minecraft, there are no parental control or privacy settings. However, there is a way to stop your child from being able to play with others.

Minecraft has two main player options:

Singleplayer: Singleplayer is entirely safe, as no one can join the player's game and no one can contact you through the Minecraft chat.

Multiplayer: This is the mode that you need to be careful of, as players can join any game they want, public or private, and can contact any player, weather they are friends or strangers.

LAN: You can also play together with friends in the same location or room, if you are all sharing the same modem via Ethernet or via WiFi.

How To Set Up LAN:
1.Log into a Single Player Game.
2.Click the "esc" button to return to the 'Game Menu'
3.Click 'Open To LAN'
4.Then 'Start LAN World'

Other players then can join you if they are playing the same version of Minecraft. They go to 'Multiplayer' and the game then searches for local games, they should see a "pop up" to join your game.

Minecraft Modes: In Minecraft, there are many different modes. (These are for both Single-player and Multiplayer):

- **Survival:** In survival mode, the player must survive against monsters and hunger. However, the monsters can be turned off by pressing escape, going into settings and turning the difficulty to 'peaceful'.

- **Creative:** In creative mode, the player is free to do whatever they want, and monsters cannot attack them.

- **Adventure:** In adventure mode, the player is not allowed to break any blocks, but can only kill monsters and animals, or be killed by monsters.

- **Spectator Mode: Y**ou can fly around and just observe, not interact with anything in Minecraft. You can fly through solid objects

Safety On Minecraft

Beware of Viruses and Malware:

Always make sure that you are downloading Minecraft from the official website www.minecraft.net or the official mobile game on iTunes or Google Play, otherwise, it is very likely that you will download some sort of virus. Do NOT download the game from any website that is claiming to be giving it away for free or is a 'torrent'.

Mods:

Additional content can also be downloaded for Minecraft through 'mods', which are small or large changes to the game that are unofficial. There is a risk that if you download one of these 'mods', you will download viruses or malware on your computer. Always make sure that you are pressing the correct download button when downloading a 'mod' from a website, as many of those kinds of websites have multiple download buttons for different software in order to be misleading and to try and plant a virus on your computer. The only way to tell if a 'mod' is really safe is if the 'mod' is very popular or if the website looks official and secure.

Child-Friendly Servers:

There are many servers in Minecraft that have been set up exclusively for families and children to play on safely. The servers have strict rules on language and behaviour, which is guaranteed by the moderators. They are also whitelisted, meaning it is impossible to connect unless your name has been added to the list, preventing random strangers from joining the server.

Some of these websites include:
http://www.blocklandia.com
http://www.sandlotminecraft.com
http://intercraften.org
http://www.autcraft.com
https://www.cubeville.org

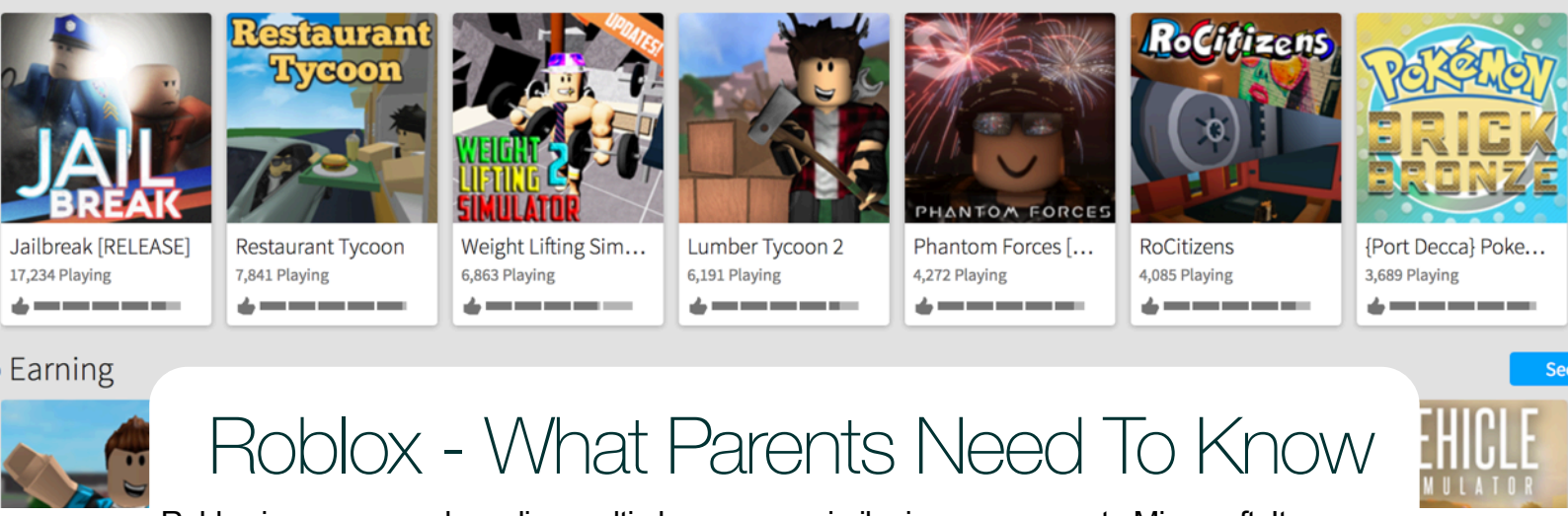
Kids Safe YouTube Minecraft Channels:
Always check before subscribing. Enable YouTube safe search settings P. 14 or Use the new YouTube Kids app.

https://www.youtube.com/user/CaptainSparklez
https://www.youtube.com/user/TheDiamondMinecart
https://www.youtube.com/user/iBallisticSquid
https://www.youtube.com/user/paulsoaresjr
https://www.youtube.com/user/MinecraftUniverse

Parental Consent:

Playing on Minecraft Realms, chatting in Scrolls, making purchases, or changing settings on the Mojang account site, is not possible now unless you have parental consent which includes verification via a credit card.

Minecraft Realms is a paid subscription service provided by the owners of Minecraft where you can host a server for friends, without having to set up I.P addresses, ports and LAN networks. Sign up create your own world and invite your friends. https://minecraft.net/en/realms/



Roblox - What Parents Need To Know

Roblox is a very popular online multi player game similar in appearance to Minecraft. It now has 30 Million active users. Roblox is primarily an online platform that hosts user/player made games. Players can choose which games they want to play. Games can be anything from navigating obstacle courses, finding your way through a spooky maze, role playing games and much more. Some games are quite scary and too violent for younger players.

Players can also build their own "worlds" or games via the Roblox Studio app. They can earn spending money called Robux or spend real money to gain Robux for upgrades and for extras. Roblox is available on both mobile devices and on P.C's.

The Good
Roblox can be creative and fun, and is designed for players to play online with each other within the games. Some of the games are G and PG rated and certainly seem suitable for younger children, but only if the parental controls are set up and there is strict parental supervision. Under 13yr old accounts have some automatic restrictions set. Privacy settings and account restrictions can be enabled for all accounts including over 13+

Watch Out For
There is a risk of stranger danger and adult content, including pornographic graphics. Roblox certainly has clear rules around no swearing and no pornography, but Roblox can only rely on such behaviour being reported. Some players are exposing children to pornography by "wearing it"

What Is The Recommended Age?
There is no age limit determined in the Roblox Terms Of Service. Roblox TOS do mention that younger children under 13+ need to have parental consent and supervision, but there is no mechanism for parental consent required for underage sign up.

Can You Play It Safety?
In March 2017 Roblox included some extra parental controls or account restrictions. You can set the account restrictions in all accounts including 13+ accounts. Parental controls are optional. An account that is listed as under 13yrs automatically has some extra privacy.

Adult Content & Swearing
Roblox already ##### out common swear words, but some players creatively get around those in other **Ways**. Rude titles, clothing with swear words and skimpy clothing also with playing Explicit Music. Roblox did introduce a filter in June 2017 to avert any nudity in the game. Games that are registered as having Mature or Adult content can be blocked in under 13+ accounts.

No Single Player Option

Unlike Minecraft, that has different modes of play, you cannot play single player offline.

Stranger Friend Requests
Whilst the new account restrictions can do a great job of blocking chat and blocking games that have adult content within them, unfortunately your children, even with the strictest settings set up, WILL still get random friend and follower requests from strangers, which they can freely accept. I received about 3 friend requests for every 1hr of game play on an under 13yr account with the available account restrictions all enabled to the strictest settings.

If your child accepts those friend requests, unless the parental controls are set to the strictest "no chat in game" settings they can then talk to these strangers, who become "friends" after their request has been accepted, via messaging and chat, they can also play with them on shared games. In my own experience there were also a lot of spam accounts sending friend requests also.

To delete friends click on your friends menu, and the click on the profile of the "friend" you want to "de-friend" and then select "Unfriend" from their profile top right. You can also report players here also for swearing, grooming, dating or asking personal questions.

Followers
Your child may also have “Followers” other players that can “follow your progress and actions on Roblox” As of publication there does not seem to be anyway you can see who your followers are in the “Friends” tab, or a way to block or stop them from following you. This is a serious oversight in Roblox.

Multiple Accounts - Ghost Accounts
There is no way to stop your child from having multiple Roblox accounts on the one device. Players can have several accounts. Your child could have one Roblox account you know about....and perhaps one over 13+ account, you don't know about, a "Ghost" Account, as they are often known as. There is no restriction or mechanism to stop your child from setting up an over 13+ account. You will not get an email notification about a new account being enabled, or be able to see it on their device if they log out of it.

Play WITH Your Kids

To really understand Roblox, it is a good idea for parents to supervise account sign up, set the account restrictions, and then sit with their kids when they are playing. For younger teens and under 13yr olds Parents are advised to set boundaries around accepting friend requests, and supervise your child if you do allow them to join and play with their real offline friends.

The Parental Controls Your Kids Won't Want...

Roblox is a very popular game for kids to play online together. Most children will want to play with their real life friends. They will be unable to chat with their real offline friends in the game if the strictest account restrictions are set up. To protect kids who can't be trusted not to accept random friend requests, or to send friend requests to strangers, you have to set the parental controls so that they cannot chat in game, or accept game invites to pay together, even from their real offline friends. They can of course use another chat app outside the game to talk whilst playing together in the game.

If you do allow your child to chat in game, and accept messages and invites to games from their trusted friends, parents need to closely supervise their child's in game friends list, to make sure they never accept a friend request from someone they and you don't know. You can set the account restrictions so that your child only communicates with vetted friends, but you cannot prevent them from friending strangers via the account restrictions.

How to set Roblox with Parental Controls

1. On sign up set your child's real age. Change it in settings to under 13yrs if they set it older.
2. Make sure your child does not use a real name, and has a strong password. No sharing.
3. Your child can set up an adult or over 13+ account on the same device, make sure your child only has one account with the correct age. Hard to tell.
4. Go to settings via “More…” or Settings icon, then Account info, provide your parent email address via “Add Email” . Make sure your child doesn't have access to your email account.
5. Follow the link in the verification email from Roblox to set an unguessable 4 digit PIN.
6. Enable Account Restrictions in Settings/Security. Default Contact settings will be locked.
7. For looser settings turn off “Account Restrictions” Go to Privacy settings and set parental controls you wish your child's account to have.
8. Turn off Notifications in settings, for extra security
9. Set social media accounts in Account Info/Social Networks to private or delete them. Also make sure your child doesn't reveal personal information in Settings/Account Info

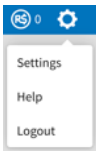
What Do The Parental Controls Do?

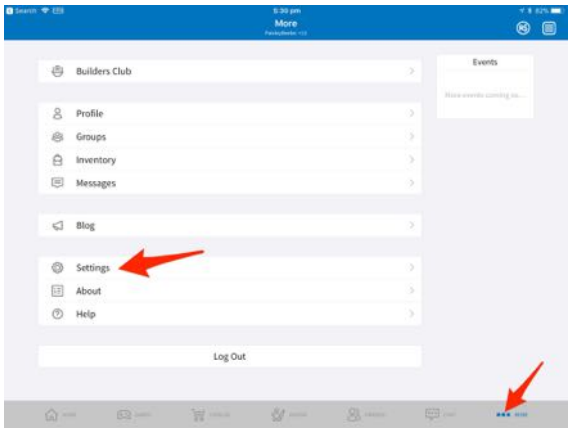
If the strictest account restrictions are set on an under -13yr old account.

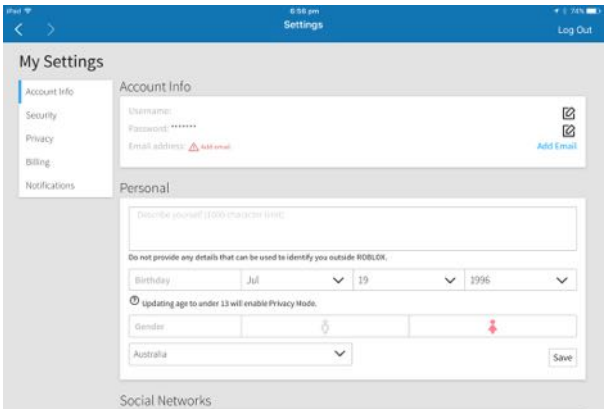
1. Your child will not see any messaging or in-game chat.
2. Your child will be restricted from joining games that have adult content such as violent games, or any games with adult themes.
3. Your child will still get random friend requests. Check the requests tab and "Ignore" them
4. Your child will still encounter other players who may push them around, but your child won't be able to communicate with them.

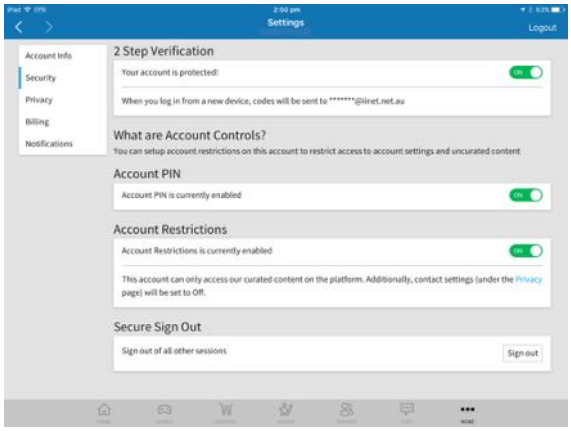
Set Parental Controls Below.

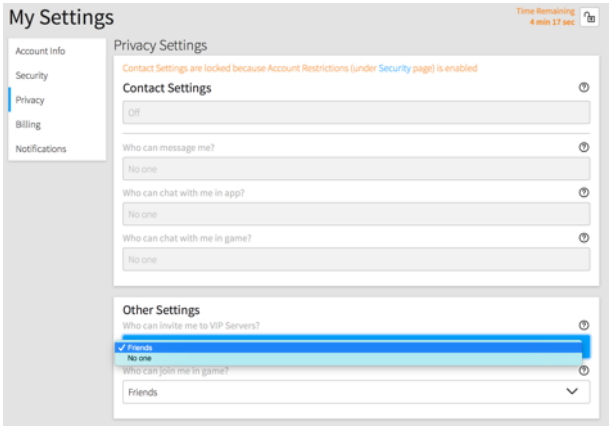
On iPad go to lower right menu click “More …." Then “Settings” “Security” “Privacy”
From a PC Web version click Settings icon top right of screen. “Security” “Privacy” “Notifications” Check all are as below. Turn notifications off. Exit out.











Parents Guide To Clash Of Clans

Guest Post Will.B

What is Clash of Clans?

Clash of Clans is a free online mobile game available on both Apple iOS and Android. It is a very popular game based around building fortress's to attack and defend against other people in Clans. This game does have some very expensive "In-App purchases, as much as $100.00. You join clans with others to play in wars against other clans. It is limited to the 13+ age group.

Can you play single player?

The game includes a single-player option. This is accessed by pressing the map button on the bottom left side of the screen, and is the map located on the right hand side.

How many can be in a Clan?

There can be a maximum 50 members in a clan, this can be changed by the clan owner.

How do the clans work?

Clans can either be public or private; in a public clan, anyone can join without invitation. In a private clan, only invited people can join.

What's the aim of the game?

There is no real aim to the game, except to attack other's bases. If you are playing singleplayer, there is a campaign which can be finished by defeating all the bases on the map. However, in multiplayer, you can play any way you want, with the majority of people competing for the top of the leaderboards, which is measured in trophies. Trophies are collected through defeating enemy bases in multiplayer and by successfully defending against enemy players.

In-App Purchases

You can play the game without purchasing anything. However, there are extensive waiting period for building, researching and upgrading to finish if you don't purchase gems.

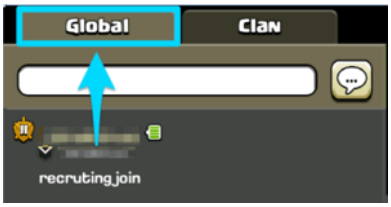
How do you win?

You cannot 'win' clash of clans. It is a persistent game, in which there is no goal or objective, unless you are playing the campaign. If you are playing the campaign; you can 'win' it by defeating all the bases on the map.

Can you play with friends privately?

No. However, the game does not force you to interact with other players, but instead allows them to attack your base and for you to attack them without interacting with them.

Can you chat privately in game?



You can only chat in a global chatroom or a clan chatroom. There is no direct communication method implemented in the game. Global chat is unmoderated so there can be swearing and adult language.

How do you stop random people from requesting to join your clan?

Set a 'required trophies limit'. This would mean only people with a certain amount of trophies would be allowed to request entry into the clan. This only applies to 'invite only' clans. This is not fail safe though, if a stranger has the required trophy level.

Do you have to complete a level to log out?

You can stop playing, as long as you are not in the middle of attacking a base. If this is the case, then you have to surrender before quitting.

What makes it so addictive?

The game is addictive because of the competitive aspect of trying to be the 'best player' or the 'best clan'.

How do you block people?

To block, tap on their name and select 'mute' from the list. This only applies to clan chat though. You can also report them for inappropriate behaviour by tapping 'report'. When the player has received seven reports, they will be banned for 24 hours.

Dangers?

The only real danger of Clash of Clans is the global chat. It is the only place where you can interact directly with complete strangers. However, it is avoidable as long as you simply ignore messages on the tab at the side of the screen.

Adult Content?

There are no parental controls, but Clash of Clans is a very mild game when it comes to adult content within the game. The only aspect that would come close to violence is attacking another clan. The language in global chat and potentially playing with strangers either adults or children is the biggest danger. There is a simple profanity filter in settings.

Finally:

There are reports of adults gaining access to private clans presenting as children to groom the children within the clan. For younger children it is wise for a parent or trusted adult to play within the clan. As with all online games where adults are allowed, there is always a risk that your child might come in contact with an adult or a child that likes to upset others in online games.

Parents Guide To Fortnite: Battle Royale 12+

What is Fortnite: Battle Royale?

It is a free online multi player survival game, with 125 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.

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 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 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. Playground mode is for exploring and testing out skins 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. Text chat in teams cannot be disabled at this time.
- The recently released mobile version of the game on iOS Apple devices doesn't have voice chat yet, but does have text chat.

- The weapons are anything from axes, swords, bombs, handguns, sniper rifles, machine guns and bazookas and self guided missiles
- You can level up and get fancy outfits and dances (emotes) by being a successful player or by paying for them. The more you play and longer you survive the more rewards you gain
- You can purchase extras in the game with a "Battle Pass" that help you level up faster and get fancier "skins" Axes backpacks or outfits. Don't allow the use credit cards to purchase use gift cards like xBox or iTunes gift cards.

Playing It Safe

Make sure your children are old enough and mature enough to cope with the gun violence and competitive nature of this game. Younger players should never play online games with strangers.

- Set a time limit for play, this game can be quite addictive, due to wanting to level up and win
- Monitor closely with younger players, you cannot lock privacy or chat settings with parental controls.
- Make sure younger players only play in teams only with real life friends
- Adult supervision is needed for younger players to ensure they don't play with strangers, and have voice chat on. Switch off in Settings/Audio. Set Game privacy to friends or private
- Voice chat can be disabled in the audio settings in the game, but if your children are playing with their real life friends may want it on
- Your child may want to voice chat using another app like Discord, make sure the privacy settings are set up within Discord Messenger go to Settings/Privacy & Safety
- Keep a close eye on the game as the developers will be adding new things to the game over time, including competitions and other means to encourage more playing
- Kids sometimes get picked on or bullied in the game if they are playing with players they don't know, this can involve tricking them or killing them over and over

Safety/Privacy Settings

Find the "Game Privacy Settings" by clicking the 3 horizontal bars top right of the screen when the game is launched. These settings block unwanted friend requests & contact from strangers.

Voice chat settings - Click setting icon top right in the game and then Audio tab to disable.

There are further settings via the "Manage Friends Tab" to add more privacy that include "auto decline friend requests" "Hide blocked players" so you don't see players you have blocked and a "Filter Mature Language" setting that will hide any bad language in text on the screen.

Block invites from strangers

Manage Friends

STEAM

Guest Post By Will.B

Are your children talking about Steam? Are they asking you to allow them to buy and download games from this gaming platform?

What is Steam?

Steam is an online game platform, where you can purchase games and download them from the Internet. They are then stored in your Steam profile, you can download them onto any computer. One of Steam's most popular features is it's trading system, which allows you to exchange items in your 'inventory' (Items that you own) for items in someone else's 'inventory' (Items they own). These items include games, trading cards and in-game items.

What sort of games can you buy on Steam?

Steam offers a variety of different games, with a large variation in price. Many of the games on Steam are child friendly, with little to no violence, but there are also many violent and mature games. In order to choose the right game for your child, always make sure to check the rating, right column on game store. (not all games have ratings, check developers website or other sources to be sure). On steam games are rated by age, e.g. 'pegi 16' means 16 or over.

Are there any parental controls for Steam?

Steam offers a content restriction setting called 'Family View' (Directions can be found on the image right). This prevents anyone from purchasing a game outright, and instead makes them enter a pin before completing the process. This is very useful if you want to restrict your children from graphic content. There is also an age restriction on many games, meaning you have to enter your age before continuing, and if you are too young, you cannot access the game. However, this is easily bypassed by lying about your age, so it is not the recommended use of content restriction.

(To find the family view setting, go to: (name)'s Account Details scroll down to Manage Family View - See Screen Shot Right)

Privacy - Blocking

Go to your account - Click your "Profile Name" - "View profile" - "Edit Profile" - "My Privacy Settings", select level of privacy to "Private' or "Friends Only". Block messages by hovering over senders profile and selecting "Block All Communication" and remove from friends list. Set everything to Private if you are getting annoying friend requests/ messages. Go to https://steamcommunity.com/chat/ through your web browser to change your chat notification settings if needed. If constantly harassed you may have to change your Steam Nick Name through "Edit Profile"

How do you pay for games on Steam?

Steam implements a useful and convenient method of paying for games, where you can either pay directly for a game, or store money on your account using your 'steam wallet'. The 'steam wallet' is very similar to a bank account (without interest), where your money is held until you purchase something with it. There are a variety of different ways in which you can purchase games on Steam or inject money into your Steam wallet, including: PayPal, Webmoney, VISA, Mastercard, American Express, Discover, and JCB

Additionally, a much safer method of payment is buying a 'Steam gift card' from a gaming retail store. There are $20, $50, and $100 cards, you will get a code that you enter into the 'Redeem a Steam Wallet Code' section of Steam (Directions below). This will then inject that money into your 'steam wallet'.

(To find the 'Redeem a Steam Wallet Code' section of Steam, go to http://www.steampowered.com/wallet and sign in if necessary. Enter your code and press continue.)

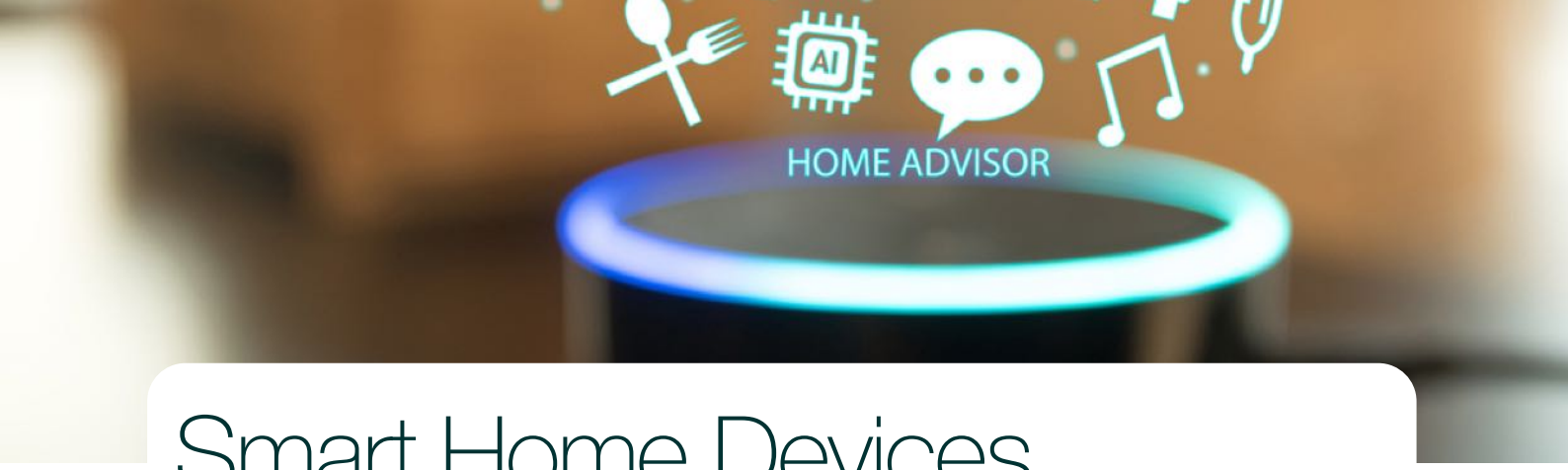
Dangers?
When it comes to Steam, there are very few dangers through purchasing games, as all of the games displayed are authenticated by Steam (personnel). However, the trading system in Steam can be easily exploited, as you can be scammed easily or receive an unfair deal. This can be easily avoided by not partaking in trading or by making sure that you are getting a good deal.

Are there any games with viruses?
It is extremely unlikely that Steam will give you a virus, Steam personnel authenticate all games, this means that they have been monitored and tested to make sure that there are no viruses being harboured within the game itself. It is not guaranteed, however, that a game will not have a virus. Always make sure that you have anti-virus software to prevent this.

Mods (Modifications, modding)
Steam has an immense community based around modding (additional game content that is used to enhance the gaming experience), and as such, there are many dangers that come within this field. No matter what mod you download, there is always a risk of it being a virus. Again, anti-virus software can help to prevent this.

Benefits
Steam allows you to store games on a cloud-based system, where you can download them at any time on any computer. This puts an end to the issue of buying new games due to buying a new computer or losing the CD. It is also very flexible in payment choice and allows for great community interaction. There are also many security measures that can be set in place to restrict content and unwanted purchases, as well as to block viruses.

Extra Security
Set up Account Security through your Account Details via "Steam Guard" so that a code will be sent to an email address or Mobile phone when logging in from a new computer or browser. This well help prevent hacked accounts.



Smart Home Devices

Smart TV's, Fridges, Children's Toys, Doorbells, Baby Monitors, gaming consoles and of course the usual computers and phones. So many devices in our homes can now be connected to the internet, but how safe are they, and what do you need to do to secure them?

Smart Speakers
2017 was the year of the Smart Speaker, with the recent release of Amazon and Google Home Speakers and now Apple Home Pod. These speakers are great for portable music streaming, but are also fun devices to use as home assistants. Completing tasks such as controlling lights, air-conditioning, shopping, security and more. Just like your own personal maid or butler.

Are They Safe, Are They Private?
Every Device in your home that connects via Wi Fi and has an app, may be also connected to the internet. Read the terms and conditions that come the device, does it share your personal data with other areas of the company or third parties? Connecting to your device via the local area network, Wi Fi or Bluetooth without connection to the internet is more secure.

Setting Security Is Essential
Can someone hack into your home smart device, or steal your personal data, which could include voice recordings, video, address details, email addresses and passwords? It is possible if you don't have security set up on the device or your connected account, or if there is some sort of data breach on the account side.

Passwords Are Vital To Protect Your Family
Set a good strong unique password when setting up your smart device if prompted. Also go to your security settings in your online accounts like Google, Apple, Amazon to see that you have a strong password. Set extra security such as two factor authentication. You will then be notified if someone is trying to access your online account from another location via email or phone.

Is the Speaker Listening To Us ALL The Time?
Smart Speakers are clearly listening for a command to start recording and listening. According to the manufacturers these speakers don't store anything they hear before they hear the trigger word such as "Ok Google" or "Hey Siri" or "Alexa"

Delete Voice Recordings & Data
Amazon Echo: App Settings/History or "Manage Your Contacts" from Amazon web account.
Google Home: go to myactivity.google.com click the 3 dots top right and select "Delete Activity By" Select date range or select products and choose "Voice & Audio".
Apple Home/Siri: Turn off both 'Ask Siri' and 'Dictation' through "settings" on your iOS device, then switch back on. Apple encrypt all your voice recordings and data so that if your data were hacked it is unreadable, even to Apple.

How To Set Parental Controls

Kids love Smart Speakers. Finally someone can answer the “Why Is the Sky Blue?” style questions that parents have been struggling with for eons. But there may be a risk to your family having an unfiltered smart device that can also transmit adult content. Asking an innocent question of a Smart Speaker and receiving an adult response is not safe.

For all internet smart devices find the settings through the linked online account or the physical controller or app, navigate to restrictions or parental controls. Search online for directions if they are not listed here.

Smart Speakers:

Google Home: Set “Family Link” to link your child’s parental controlled account. Search online.
Apple Home Pod: Settings/General//Restrictions on your connected apple account or device.
Amazon Echo: No parental controls other than a pin code for purchases.

Smart TV’s:

Check the device manual or search online for the manufacturers website. Explore the settings through your devices controller or connected app.

Apple T.V: Switch on Apple T.V. From home screen go to Settings/General/Restrictions

Chromecast: Set restrictions on connected devices & apps. i.e Netflix, Apple iTunes, YouTube

Fetch T.V: Home screen/settings/parental controls or guide https://www.fetchtv.com.au/faqs

Gaming Consoles: Xbox, Playstation, Nintendo Switch all come with parental controls. You can restrict messaging, profiles, certain games and in App Purchases. Check settings, through the device or search website or the manual.

Media Apps On Smart TV’s

Netflix Click the the “Kids” profile at the log in screen and configure. You can put a pin code on other Netflix profiles to prevent your child accessing them.

Foxtel: Go to settings and parental controls on Foxtel, and set up a parental controlled account

YouTube: On your smart T.V navigate to the YouTube app then “Settings” and scroll across to “Restricted Mode” and tick enable.

Top Tips For Securing Your Smart Home Devices

- Set strong passwords and two factor authentication for Amazon, Google, iTunes accounts
- Use Google Authenticator or Sophos Authenticator app rather than phone number, for two factor Authentication.
- Set strong passwords for your devices, hard to guess, no personal details. Over 8 digits.
- Set unguessable pin codes, not 0000 or a code that relates to a birth year or date.
- Set a strong password for your Wi Fi router. Check manual or search online for instructions.
- Activate firewall settings for your modem and computers. Keep anti virus up to date.
- Keep passwords offline in safe location or use password manager i.e 1Password - Lastpass
- Restrict personal details when setting up your device. No street address, phone numbers.
- Set firmware or software on devices to update automatically if that is available. Check every 6 months or so to see if your device or modem requires a firmware update.
- Delete your data - voice recordings from the cloud from time to time see above.

Where Are Kids Going Online?

Supervise Without Spying!

One of the most important things when raising teens and pre-teens 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. 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 install a parent control app, like Family Zone or use other available parental controls, being open and honest about monitoring your child's internet use is essential. "Spying" 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.

How To Be More Aware

Keeping computers and digital devices in a central part of the house is the first and easiest step to being more aware of what your kids are doing online. Treat digital technology much like the TV, (unless of course you have TV's in the bedrooms!) Sit with younger children when they are using devices so that you can help them navigate the device safely.

If you are able to casually walk by or glance over your child's shoulder you should be able to supervise older children surreptitiously. You can then ask some questions about what they are playing or writing, make sure you show interest in a positive way not just in a concerned way. Keeping devices within sight and hearing distance is essential to be able to keep an eye or ear out for anything that sounds like your child is possibly upset with what they are seeing online. Supervision and genuine interest is key here, and have FUN!

"Spying" is sneakily following your child's digital interaction without openness or honesty, and can lead to resentment and distrust. If you use device monitoring software be open and transparent about why, and how it is used, and when monitoring might end. Point out the positive aspects of supervision. Equate it to offline supervision and parental responsibility.

Here are some suggestions for some fun things to do with your kids on computers or portable devices.

- Share funny videos
- Find a game that you can play with your child (see suggestions in this manual)
- Share articles with your kids about their favourite games
- Find a Wii game or console game (Xbox - Playstation - Nintendo) you all like play
- Follow The Cyber Safety Lady on Facebook or Twitter, subscribe to my blog for ideas.
- Have fun with some educational apps, www.commonsensemedia.org has suggestions
- Download a drawing app like "Brushes" and do some drawing together on a tablet device.
- Share an interactive book like "The Fantastic Flying Book"
- Get your kids to teach you a game, like "Roblox" "Fortnite" or "Minecraft"
- If you see them playing a game, just ask questions about it every now and then, (be careful about this one, if you interrupt at the wrong time, they might get frustrated!)
- Make sure your child's friends feel welcome to come over to all play a computer game together, so you can find out what the other side of the conversation sounds like (if your child wears headphones you may only hear one side)
- Check out some of the game recommendations in this book
- Buy my new cyber safety manual every few years to keep up to date
- Come to a Cyber Safety talk every year or so. New information, new apps!

Go with your kids to the Gaming stores to help them choose suitable games.

Cyber Bullying What To Do?

Cyber Bullying is repeated cruel behaviour used to intimidate, embarrass and harass over telephone or internet connection. It can be anything from name calling to uploading embarrassing photos, impersonating accounts, posting private information or photos of you or your family online. It can also be interfering with your content in some way online without your consent and in such a way to harass.

How To Deal With Cyber Bullying:

- Block the cyber bully (find the blocking tools on each software) This cyber safety manual shows some of the blocking tools for some apps.
- Keep evidence of the bullying by copying the content and saving it before it can be deleted. If on a Windows computer take a screen shot by clicking the Prt Sc SudRq Key (usually top right 3rd key from right on any Windows Computer) or search for the “Snipping tool”. On a Mac hold down Command-Shift-4, then select an area: Take a screenshot of the abuse and save it. Use a separate camera if unable to screen shot.
- If it's by SMS don't delete the messages. You can take screen shots on most smart phones by clicking the off/ on switch and home or volume up button simultaneously for a second.
- Report the cyber bullying to the platform it has occurred on via the reporting tools and a trusted adult or person of authority.
- Do not retaliate in anyway, in person or in text. Don’t share or repost the abuse to shame the abuser.
- If the abuse is illegal (stalking, threats of violence) report it to your local police, your ISP or telephone provider. For Adult victims report serious matters to http://acorn.gov.au

How To Report:

If in Australia you can contact the Australian Government organisation eSafety.gov.au to report cyberbullying and to source further advice.

Report to school if it involves another student, or even a student from another school .

Death threats, stalking, harassment are considered illegal, and should be reported to police.

Check up on your legal rights in regard to cyber bullying from http://www.lawstuff.org.au

It is important to know that each state and territory in Australia has different laws for bullying. Lawstuff provides legal information to children and young people in Australia. Please check your State or Territory to get legal information related to Cyber bullying in your area:

Kids Helpline has 24hr phone help.
Kids Helpline - http://www.kidshelp.com.au/teens/ or phone 1800 55 1800

Bullying No Way - http://bullyingnoway.gov.au

For Cyber Crime, hacking, scams report to http://www.acorn.gov.au

To report scams go to http://www.scamwatch.gov.au sign up for their alert emails.

4 Most Important Tips For Parents

To Prevent Cyber Bullying

1. Supervision

You can't effectively supervise your children on digital devices behind closed doors, out of your eyesight and out of earshot, (iPads and smart phones are computers too!). Digital devices should be used in a central location in your residence for effective supervision. This is the number one cyber bullying prevention tool. You need to be able to be there on the spot if your child gets a nasty message on social media or via a message. Often their physical reaction to what they are reading will alert you to a problem, well before they tell you. Create a safe harbour for your children to report upsetting online behaviour to you.

2. Education

Check with your school to see if your children have been receiving any Internet safety talks and what subjects those talks have covered.

If you, as a parent or carer, are given an opportunity to attend a talk on cyber safety, cyber bullying or digital parenting, it is very important you find the time to attend, even if you think you know it all, you may learn from other parents or even may provide support. Encourage other parents to attend, then you are all on board for shared safety.

If your children have not been given any education about cyber safety at school, then contact your school and suggest it. My own cyber safety talks are available to teachers, students, parents, grandparents, childcare workers and youth workers.

3. Security

If your child is ever cyber bullied you need to understand what security measures can be implemented to prevent the cyber bully from ever contacting your child again. Firstly make sure you have basic privacy and security settings in place, this book has many of the necessary tools. it is important you don’t simply just cut your child off from their friends online.

Make sure your digital devices, computers have up to date software and an anti-virus program is set up to do regular virus update checks. Then make sure all the available privacy settings are set up on any application your child uses to communicate with others including online games, Skype, Messaging,Video Messaging, Online games, Social Media, YouTube and email. You and your children need to know where the blocking and reporting tools are on each application, to be able to protect your child. They may have to shut accounts down and set up new ones.

Make sure your child is not using their real life name online for messaging apps or online games. Get them to use pseudonyms, and different names per app.

4. Online Behaviour

Be sure your children are not using adult apps, ensure they are using age appropriate games and social media. Younger children are at higher risk of cyber bullying, they simply don’t have the online street smarts of older children.

Ensure your children don’t contribute to cyber bullying, supervise them openly and closely online without spying - unless absolutely necessary. Use parental monitoring software like Family Zone with younger children, be open about what the monitoring does. Check your child’s device with your child for browsing search history and unsafe apps and behaviour.

Share messaging accounts with your child if possible when they are younger. Skype does this well.

Sexting & Sharing Nudes - Getting Help

Sexting is sexual texting. The sending of sexual or nude pics or video via SMS or Messaging.

It is illegal to take or keep a sexually explicit or nude photo or video of a person under 18 years of age, or to share it with others, in person or via messaging.

"It's No Big Deal!"
Many teens see sexting as flirting or as a joke, and don't understand that if reported, they may be charged with possession or sharing of child abuse material. In some states a teen may end up being charged and could be listed on the sex offenders registry. Different states have different laws around under age children taking and sending nude or partially nude photos with consent. www.lawstuff.org.au has the latest laws around sexting for each state.

The other consequence of sharing or taking sexual or unclothed photos is that the photo may end up being seen by persons not originally intended. In some cases phones and online photo apps have been hacked, and images never intended to be shared, have subsequently been posted online in image forums along with names and locations of the victim. Teens who think their nude photo/video has been shared without permission should report to a trusted adult as soon as possible to stop the spread. You can also report to eSafety.gov.au to assist with removal and report to your local police. Police may not press charges against the victim for sharing a sexual image that was then shared on to others.

What Should You Do With It?

If you see or are sent an inappropriate photo/video of a person under 18years of age, you should report it, and delete it. Keeping such a photo in your possession without reporting it to the authorities may result in charges. Report it to school, if you suspect it was sent from another student. Delete it, never share it on, or screen shot it. If you view it on social media also report it to authorities.

"Revenge Porn"
The sharing of sexual or nude images of another person without their permission is known as revenge porn or image based abuse. Image based abuse is illegal and a form of harassment. Report to police or get help here https://www.esafety.gov.au/image-based-abuse

Being Asked For Nudes

If a young person under 18 years of age is asked to send a nude or sexy photo or video of themselves it is very important that the person asking for the photo is reported to a trusted adult and the police. It is important that this person is stopped and prevented from asking others for the same. Schools and the police need to be told if an underage person is being asked for rude or nude photos. It is against the law to ask for images or video of a sexual nature from a person under 18years. Be sure to block the person to prevent further contact.

How To Report:

Report to your school and the local Police. It can be up to the discretion of the police as to how the matter is handled depending on the circumstances. eSafety.gov.au can help you have pics removed if they end up on a social media platform or a website.

Each state and territory in Australia has different laws for sexting and revenge porn. Check your State or Territory to get legal information related to sexting in your area:
http://www.lawstuff.org.au

Screen Time Tips

New screen time limits as recommended by the American Academy of Paediatrics 2016

- For children younger than 18 months, avoid use of screen media other than video-chatting. Parents of children 18 to 24 months of age who want to introduce digital media should choose high-quality programming, and watch it with their children to help them understand what they're seeing.
- For children ages 2 to 5 years, limit screen use to 1 hour per day of high-quality programs. Parents should co-view media with children to help them understand what they are seeing and apply it to the world around them.
- For children ages 6 and older, place consistent limits on the time spent using media, and the types of media, and make sure media does not take the place of adequate sleep, physical activity and other behaviours essential to health.
- Designate media-free times together, such as dinner or driving, as well as media-free locations at home, such as bedrooms.
- Have ongoing communication about online citizenship and safety, including treating others with respect online and offline.

Screen Time Limits

Ideally your children should be starting to start self moderate their own screen time when they are upper years in high school. Teens need to be able to switch off from screens to do other things by themselves. The more children rely on their parents to tell them to switch off, the longer it will take for them to learn to self moderate. Children that have reactive parents rather than a routine and a plan for screen time limits, will continue to rely on parents to remind them.

All Quiet In The House

Excessive screen time can have a dangerous payoff for many families, everyone is happy if they are all on screens, no one is fighting or getting under your feet. Be careful your family doesn't get lulled into this seductive scenario. Some healthy conflict in families, whilst uncomfortable, is necessary to learn teamwork, compromise and resilience.

Digital Parenting Is NOT Different!

Many families don't seem to treat screen time issues the same as they do other boundary issues in families. Some families have one approach to digital parenting, and an entirely different approach to other family boundaries. Families need to set boundaries around screen time in the same regard as they do with any other behavioural issues.

Parents are often struggling to understand the digital technology their children are using, and are trying to work out how to limit its use in a reasonable practical way. With education comes power, make sure you are really up to date with how your children are using apps and the internet. When you know how the technology works, which apps are suitable, and how to use the technology to help you moderate, then you can make educated, informed decisions for your child.

Understanding Parental Controls And The Technology

If you understand how the technology works, it is much easier to moderate and restrict. You can set digital restrictions around apps and screen time and also decide where the device can be used and when. Parental control apps and some built in settings enable digital switch off scheduling. Use auto switch off and timers sparingly when all else fails, it is better to teach children to develop good screen time habits and respect for boundaries for the longer term.

Digital Technology Is Here To Stay!

Kids use technology and the Internet quite differently to most adults, some would say that they are very "tech savvy", but "tech savvy" is quite different to "life savvy". Don't mistake great technical skills for life skills. Children need parental advice and supervision both offline and on.

If your child is managing to live a healthy life, maintain friendships, spend time in the fresh air and keep up with school work, don't worry if it seems they are always on their device, it's a different world, just look at the adults around you! We just can't compare our childhood with our children's it's such a different environment now.

Screen Addiction: Be clear on what your issue is.

Is your child's problem a serious screen addiction or just a bad habit?

Are you finding it impossible to get "through" to your child, are you bewildered as to how to set boundaries around devices? Your child may not be actually "addicted" to technology, but is simply doing what they want to do. **Note:** True addiction to screen time may be an indication of a more serious underlying issue. See more about that below.

More often than not it can simply be bewilderment with how kids use digital devices and parents inability to moderate them that is often the real issue, not a serious addiction. If your child is simply ignoring your concerns, it could be because they don't have a strong enough incentive to follow your limits. Rewards for sticking to boundaries works more effectively than punishment.

Let's Unpack This

- Do you really know what your child is doing on their device?
- Do you know how safe the apps are that your child uses?
- Are you being consistent with your boundaries?
- Do you give in too easily for a quiet life?
- Do you swing between harsh punishment and throwing your hands up and giving up?
- Are you and your partner both on the same page with your child's technology?

Being consistent and united with other adult members in your family about screen time boundaries is absolutely vital. If your child is confused about what the rules are, and what the consequences are for breaking them, they won't learn what they can and cannot do. They will often then push those boundaries to see if they get the "I give in" approach that day, or the over the top "That's It I'm Throwing It Out" approach.

When To Seek Professional Help

Excessive screen time can be a sign that something is very wrong with your child's well being. Spending all day and night in a dark room with only the light of an LCD screen can be a perfect hiding place for a teen who is being bullied at school, or is struggling to deal with mental health issues, or family dynamics. If you are finding that screen time is becoming a huge issue for your family, don't put off seeking professional advice.

Stop Talking And Act!

Many parents think that “reasoning” with their child, (over and over) or getting an expert to speak to their child, should be enough to convince the child that they are spending too much time on screens. It is very important that you do have open conversations around the health issues of too much screen time with your child, but when all is said and done, you may have to stop the reasoning, the begging, the shouting and the threats, and simply set your rules and consequences for breaking them in a planned and methodical way. Ultimately, you can pull rank, you are the parent and the provider. You have to be the boss.

I Can’t Keep Up!

Screen time limits shouldn’t be about trying to constantly outsmart your kids, it should be about teaching your children to take responsibility for their own devices and screen time so that they have a balanced successful life. Certainly parents do need to learn how technology works to a degree, in the same way that you need to understand all sorts of other things that your children like to do. Avoiding education around digital technology and hoping for the best, is a recipe for disaster, and many children rely on the fact that their parents are ignorant about apps and digital devices, to get away with doing things they really shouldn’t be doing. Self moderation on screens takes time, and children need a lot of guidance to learn how to organise their time, and learn discipline to switch off when needed. Be prepared for lots of whining, begging, pleading, shouting, schmoozing and bamboozeling! Yup just like a toddler….all over again!

Families Need To Work Together On This!

Family time without screens is so important, too much screen time, can mean that we aren’t really talking to each other or spending time in a productive way. Make some agreements around not having digital devices at the dinner table. (Have some dinners together face to face!) Set times for screen time and times for switching it off for the whole family. Model balanced screen time behaviour. Find family activities, and leave mobile devices at home or in the car.

Family digital device detox? Give up screens for a weekend to see what happens. Sometimes families need to go without digital devices to see what else we might like to do?

How To Balance It All

Screen time is all about balance. It is also about what is being done on the screen, not just the amount of time.

- Is it an educational game, or a strategy game?
- Are they using their computer to create something?
- Who are they talking to?

Ideas For Creativity On Digital Devices:

- Creating/editing movies, or stop motion animation
- Drawing with a drawing tablet or drawing program on a tablet
- Reading or writing a book or journal
- Photography or composing music
- Creating a comic or cartooning
- Learning to code, or creating an app or a game
- Building a blog or website
- Collaborating with others on a project

Set A Digital Time Table

Collaborate with your child on a routine, explain that they need to start to get things in order so that they can have time to do all things they need to do. Suggest that it might be nicer to not have mum or dad yelling at them to get off their device all the time.

Negotiate a schedule for social media time, gaming, YouTube, for example, for each afternoon after school. Half an hour to an hour is reasonable, and then stick to it. If your child wants to go over the time allotted, suggest that the extra time will then be deducted from the next screen time allotment. Take a note of any overtime. If you are consistent your children will get the message that you are serious and consistent with your boundaries. You can of course re-negotiate anytime to fine tune it, and will of course need to adjust it as they get older.

Set allowances for screen time for weekends as well. It's easier to set times to a routine, for example from 7am – 10am rather than set an overall time limit for the day, which can be split up and hard to track. Again, if the kids want to go over the limit, simply tell them that the overtime will be deducted from their next screen time allotment. Use rewards for sticking with time tables. It should only take a few days of this routine before they realise that they have real consequences for not sticking with agreed times.

Stay The Course!

You may face all sorts of resistance to these changes, particularly if you have never attempted them before, or have given in previously. If your child resorts to tantrums or threats treat the outbursts just as you do normally for this kind of behaviour. Beware the threats of rebellion, the "You're the strictest parents ever!" routine, and the sneaky "iPad under the covers" routine. If your child protests to the effect of "all my friends are allowed to use screens as much as they want!" (that old one), ask for names and phone numbers, offer to do a survey, kids usually back down at this point. If you do catch them sneaking around the boundaries, take time off their digital allotment, or perhaps confiscate the device for a short time. Reward good behaviour.

Removing or locking down the digital device for a short time if there is a lack of cooperation can help, but don't go overboard and ban everything for ever. Remember, set small consequences, else you will have no where to go if you need to up the ante. Rewards work better than punishments.

Track Family Screen Time

Keep a diary for a week of the family screen time usage, including your own. Apple now have "Screentime" to track your device use also with weekly reports. Set a weekly limit for every member of the family if needed. Get the children to help you switch off! If the kids feel everyone is on board it might help. Remember though, you are the parent, and you don't have to stick to kids' rules. One rule for kids and one rule for parents, age does have its privileges.

Rewards Are Better Than Punishments

Give rewards for times adhered to, and good behaviour on devices. The rewards could be an iTunes gift card, or work towards something bigger with points. Use a chart with points given for every day the time table is adhered to. A "star chart" for younger kids works really well.

It Does Get Better!

If you are consistent, level headed, united, fair and plan this strategy well, eventually your kids will get into a routine where occasionally they might try to negotiate with you for more screen time, (it's up to you if you comply, but beware the slippery slope!) but in general they will know the rules, as they do for every other aspect of their lives. They, and you will then enjoy far less drama in the house over their screen time use.

Family Games

Playing video games with your children is a great way to find out what they love about gaming. It also helps to open up conversations around computer games and should help kids feel more comfortable to confide in parents about what they are experiencing on various games, and guess what? You might even enjoy it!

Try first before playing with your child, age ratings are only a guide. Some 4+ games are loved by older teens, and some 12+ games might be too scary for a 12 year old.

Recent studies show that playing puzzle and quiz type video games can increase your mental agility and can help delay dementia, so get clicking!

Ages 4+

Contre Jour HD: iTunes - Google. Stunning side scroller. Cute creature jumping from blob to blob
Colour Zen: iTunes - Google. Colourful intuitive puzzle game with soothing music
Botanicula: iTunes - Google. Cute characters adventure game, beautiful graphics and music. Not scary!
Brushes: iTunes. Painting app. Beginners through to advanced artists
Monument Valley: iTunes - Google. Stunning puzzle adventure game. Apple Design Award Winner
Interlocked: iTunes. 3D wooden interlocked block puzzle. Challenging with great graphics
Minecraft - Pocket: iTunes - Google. Full version - PC - Console. Creative sandbox building game. Single player recommended for younger players
Tengami: iTunes - Steam. Japanese popup book, atmospheric adventure game. Stunning music/graphics

Ages 9+

Badland iTunes - Google - Steam Atmospheric side scrolling action adventure. Some nasty circular saws
The Room versions 1,2,3 : iTunes - Google - Steam Stunning 3D physical puzzler and Mystery game
Zen Bound: iTunes Japanese Meditative puzzle game, binding rope around pretty wooden puzzles
Gravity Ghost: Steam. Sprite flying through the universe landing on planet collecting flowers

Ages 12+

Lily: iTunes - Some in-app purchases, but no real scary things. Stunning graphics and characters
Machinarium: iTunes - Google - Steam Puzzle side scroller game. Beautiful graphics, cute characters
The Cave: iTunes - Google - Steam Adventure side scroller. Stunning graphics challenging tasks
Roblox: Online maze, obstacle course game. Chat rooms & scary murder scenes. Use parental controls
Framed: iTunes. Award winning narrative based puzzle game, Pretty Film Noir style
Superbrothers Sword & Sorcery: iTunes & Google - Steam Exploratory Action Adventure.

Ages 13+

The Stanley Parable: Steam. First person exploratory game. No violence - mild cursing via voice over.
Lifeless Planet: Steam Lost Astronaut Puzzle walking simulator game. Beautiful challenging.
Fortnite: Battle Royale: Shooter game last person standing: Guns, weaponry, minimum gore.

Ages 17+

Firewatch: Steam Mystery first person narrative. Some scary scenes, moderate swearing beautiful graphics.

More suggestions at http://thecybersafetylady.com.au/category/family-game-reviews/

Kids As Young As 3yrs Need Cyber Safety Restrictions Now!

Just when you thought you could put off cyber safety issues until your children grew into teens, parents are finding out the hard way that teens aren't the only ones with internet computer cyber safety problems.

Tots On Smart Phones

Digital mobile devices are being used by children as young as 2 years old, but some parents are still thinking that cyber safety only applies to teenagers on computers.

Parents, you had better catch up quick! Technology is moving faster than you can adjust your mindset, and if you continue to keep thinking you don't need to worry about cyber safety for your younger children until they are teens, you and your children are sadly in for a nasty shock.

Phones, Tablets, Consoles And Other Mobile Devices Are Computers Too.

Smart phones and tablets like iPads, Smart TV's and consoles like Play Station, Nintendo and Xbox are computers too, and all can be connected to the internet. Each device may have apps like messaging, Netflix, YouTube and Browsers with access to search engines. Most have the ability to download adult content through apps.

Any parent that leaves one of these devices around the home unlocked, or gives one to their child before securing it with proper filters and controls, is leaving their child open to content that may be beyond the child's ability to cope with. Take your eyes away for one-second and your child might see something that cannot be unseen, often after searching for something innocent.

Primary Schools Are Including Computers Or Mobile Tablets In Their Curriculum

Most schools are already including computer use in their primary school curriculum, students already know how to use search engines BEFORE they get to high school, not to mention underaged use of adult social media platforms.

Have parental controls and adult content filters been recommended to you for your child's BYOD (Bring Your Own Device) for home use? If your school hasn't set up safe search filters on your child's device for home use, then you may need to enable them on the device yourself, do you know how? Find out what the school has put in place, and whether it covers home use also. What can you set up for home that will be compatible with school use?

As a Cyber Safety Educator and consultant, I hear the same terrible story over and over again, how a parent didn't know how to set up adult content filters on their home internet and devices and their younger child was then exposed to pornography or sick violence, simply by searching for an innocent search term through a search engine on their computer or device.

Your Child May Not Have A Smart Phone But What About Their Friends?

Your child may not yet have their own internet connected device, but what about your child's friends. Cyber safety is a community issue, your child might be exposed to something nasty via a friend with such a device brought into your own home. Setting up an adult content filter on your home WiFi will help protect guests also. See if your Modem has parental control settings or your internet company has filtering maybe try a Family Zone filtering box.

Many parents don't even have a screen lock password on their phone or mobile device and they leave them lying around the house, only to be picked up and used by their child without their supervision. How safe is your child's friends house?

Parents are understandably concerned about the cyber safety awareness of all families in their community. Parents need to have more conversations together around cyber safety to keep all kids safer online. Encourage others to seek education around cyber safety.

You Can't Watch Them 24/7

Ask your children to respect your boundaries around gaming and apps no matter what house they are visiting, in the same way as you would expect them to maintain your boundaries around any other type of behaviour no matter where they are. Giving your child some strategies for opting out of unsafe online behaviour or unsuitable video games is essential to cope with peer group pressure. Even if they have to call you to come and collect them. Encourage disclosure.

Prevention Is Better Than Cure, What Is Seen Cannot Be Unseen

Filtering and safety settings help protect your child especially from accidental exposure to adult content. You may not be able to protect your child 100% of the time, but doing nothing about filtering/blocking adult content means your child will definitely see adult content sooner rather than later. If a child has discovered adult content and is determined to get around settings, then parents need to approach the issue as a compliance and discipline issue. Ignoring or flouting rules, breaking digital boundaries should be treated the same as any other non compliance.

Discussing Adult Content With Your Child

Make sure your child feels safe to tell you when they see anything rude or upsetting online. Make sure they don't feel as if they are in trouble. Don't ban everything if they do see pornography, get advice for setting up adult content filters. The Author Holly Ann Martin https://www.safe4kids.com.au has some great books that can be read with children on adult content and how to process it. She also gives parents advice on how to talk to children about adult content.

Filtering Options:

Explore the option of enabling filtering on your modem or computer.

Family Zone Modem Filter Box And Mobile Parental Controller www.familyzone.com

Apple and Windows PC Parental Controls featured in this manual

Google/Bing/Yahoo Safe Search Option featured in this manual

Apple Mobile Parental Controls featured in this manual

Contact your Internet Service Provider in regard to more Parental Controls or filtering options

Computer Agreement - Sample

Family Computer Use Agreement:

Mon-Fri Times:.....

Saturday Times:.....

Sunday Times:.....

Holiday Times.....

Time Limit on Social Networks:.....

I will agree to these conditions of computer use. I understand if I break these agreements or part of them, that I will lose time on my device as a result. I agree to let my parents know if I'm ever worried about cyber bullying, strangers or adult approaches . I agree to behave responsibly with regard to personal privacy online. I will only friend my true friends, and will make sure all my privacy settings stay set up. If there are any virus warnings, or changes to my privacy settings I will let my parents know. Sticking with this agreement may result in rewards, but most importantly will see me and my family safer online.

Signed:.....Signed.....

Sample computer use agreement between parents and children

Online Jargon

- LOL - Laugh Out Loud
- ROFL - Rolling on the floor laughing
- ROFLMAO - Rolling on the floor laughing my A...Off
- LMFAO - Laughing my F....in ar... off
- BRB - Be right back
- AFK - Away from keyboard
- WTF - What The F.....K
- WTG - Way to go
- Teabagging - jumping on another player with rude bits on their face....I know disgusting!
- Owned/Pwned/Ownage - I beat you!
- Pron - Porn
- Lag - slow screen on game
- Logging - closing down game
- I.M - Instant Message
- LOLOLO - laughing a lot
- GTFO - Get the F....K Out
- OMG - Oh My God
- OMFG - Oh My F..... God
- ATM - At the moment
- BFF - Best Freinds Forever
- BTW - By The Way
- CYA - See Ya
- Oder - odering Online dating as in O.D
- CU - See You
- Cyber - Sex over the internet
- FFS - For F....ks sake
- FU - F...K you
- FTW - For the win, He/She won
- FYI - For your information
- Handle - made up gamers name
- IDK - I don't know
- IMO - In my opinion
- Lulz - like LOL but meaner
- MMO - Massive Multiplayer Online Game. (like World of warcraft)
- WOW - World of Warcraft
- NSFW - Not safe for work, rude!
- O Rly - Oh really?
- PAW - Parents are watching
- POS - Parent over shoulder
- POS - Piece of Sh.....t
- POV - Point of view
- STFU - Shut the F....Up!
- THX,TX - Thanks
- TTFN - Ta Ta for now
- WB - Welcome back
- WTH - What the hell
- ZOMB - Oh My God said with sarcasm.

Leonie Smith "The Cyber Safety Lady" Can Help!

'Peace of mind' cyber safety solutions for students, teachers families, community groups and business.

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!

Invite "The Cyber Safety Lady" to speak at your next event!

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.

- 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
for some great step by step videos

“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