

USING PARENTAL CONTROLS

There are lots of ways of limiting what content your kids can see online, which apps and programs they can access and how much time they can spend online. What tools are available depends on what kind of device they're using, and what browser they use to access the web.

INTERNET PROVIDERS

Many Internet providers provide tools and services to help you manage your child's online experience. Check with your provider to see what they offer that will allow you to block different sites, monitor your kids' online activities and set times when the Internet is not available.

OPERATING SYSTEMS

Operating systems are the “toolbox” that your computer, phone or other digital device uses to run programs and apps.

Android

On Android phones and tablets, you can set what [content rating](#) you want your kids to be able to access. Android allows you to set different content ratings for different types of content (movies, books, music, games, etc.) For information on how to do this, see <https://support.google.com/googleplay/answer/1075738?hl=en>.

Android and Chrome OS also allow you to use the Family Link app if your children already have a Google account, which gives you more direct control over what content they can see and how much time they can spend using the device. For information on how to do this, see <https://families.google/familylink/>.

Apple

On iOS devices like iPhones and iPads you can disabled different features (like Camera and AirDrop), prevent your child from making in-app purchases, block access to content with specific ratings, block access to websites with adult content, and adjust privacy settings such as whether apps can share your child's location. For information on how to do this, see <https://support.apple.com/en-ca/ht201304>.

Windows

On computers, phones and tablets running Windows you can prevent your child from accessing content above a certain age rating, require them to get permission from you before buying apps or making in-app purchases, and limit how much time they spend using the device. For information on how to do this, see <https://support.microsoft.com/en-ca/help/12413/microsoft-account-what-is-family>.

BROWSERS

Browsers are the programs your computer uses to access websites. Your computer may have more than one browser installed, so make sure that you have set the parental control options you want on all of them.

Chrome

Parental controls for the Chrome desktop browser can be set using Family Link.

On the Chrome browser for tablets and mobile phones, you can turn on SafeSearch, which blocks explicit images, videos and websites. For information on how to do this, see <https://support.google.com/websearch/answer/510> and click on “Android.”

Edge

Edge’s parental controls are set using the general controls for the Windows operating system.

Firefox

Firefox does not have any built-in parental controls. However, when used on a computer using Windows 10 it will reflect the parental control settings you have chosen for that operating system. You can also install third-party add-ons for a variety of parental control functions: <https://addons.mozilla.org/en-US/firefox/search/?q=parental+control&cat=all>.

Safari

When using Apple’s Safari browser on a desktop Mac, click on the Apple icon and then select System Preferences. Choose the Parental Controls icon and then choose which account you want the settings to apply to. Click the Lock icon at bottom left and enter your password. Now you can set content rules for apps, websites and app stores. (If you want to know how to create an account for your child, see <https://support.apple.com/en-ca/HT201084>.)

SEARCH ENGINES

Search engines are the tools you use to find websites. Any search engine can be accessed through your browser, and some can also be installed as apps on a mobile device. Most browsers and devices have a default search engine that they automatically use for searches.

Google

If you have a Google account you can turn on SafeSearch, which blocks explicit image, videos and websites. You can also lock SafeSearch to prevent someone else from turning it off (though they can turn it off if they log into a different Google account). For information on how to do this, see <https://www.google.com/preferences>.

Bing

Bing has three levels of Safe Search: Strict, Moderate and Off. You can select the one you want at <https://www.bing.com/account>.

DuckDuckGo

DuckDuckGo has three levels of Safe Search: Strict, Moderate and Off. You can select the one you want at <https://duckduckgo.com/settings>.

VIDEO SITES

One of the most popular online activities for kids is watching video. Here’s how you can limit what they can watch on two of the most popular video sites – whether they’re visiting the website with a browser or using an app on a mobile device.

Netflix

Netflix lets you set parental controls to require anyone to enter a 4-digit PIN of your choosing before watching content above a particular maturity level. (The available options are Little Kids Only, Older Kids and Below, Teens and Below and All Maturity Levels.) You can also create a separate limited profile for your kids, but keep in mind that they can leave this just by clicking on Exit Kids. For information on how to do this, see <https://help.netflix.com/en/node/264>.

YouTube

If you have a Google account, you can set YouTube to Restricted Mode, which blocks some inappropriate content and also prevents you from seeing comments on videos. For information on how to do this, see <https://support.google.com/youtube/answer/174084>.

If you're using YouTube Kids, you can also block specific videos and channels. For information on how to do this, see <https://support.google.com/youtubekids/answer/7178746>.

GAME CONSOLES

Switch and Switch 2

Start by downloading the Nintendo Switch Parental Controls App. With it, you can set screen time limits for different days and set the content level you're comfortable with for game. You can also approve and review your child's Switch friends (people they can play online mutliplayer games with) and GameChat friends (people they can chat with while playing

multiplayer games.) Someone has to be a Switch friend before they're a Game Chat friend. If your child tries to start a video chat, you will get a notification on this app and can approve or deny the video call.

The settings you select will automatically apply to the Switch 2 so long as you use the same Nintendo account.

Xbox

Start by downloading the Xbox Family Settings app. Child accounts have multiplayer and communication settings blocked by default, but you can change those if you want our child to be able to play multiplayer games. Online multiplayer games cannot be played unless you have an Xbox Live sign-in.

Playstation

You can choose a "privacy profile" for your child's Playstation account: Social and Open, Team Player, Friend Focused or Solo and Focused. The last two are most appropriate for children. You can also click "Review and Customize" to choose more specific settings. "Friends Only" is the best contact level.

GAMES

Roblox

It's important to give your child's right age when registering because different features, like chat and social spaces, are only available to players 13 and up.

You will need a Roblox account that's linked to your child's account to be able to manage parental controls.

To link your accounts, start by selecting the gear icon (on desktop) or More and then the gear icon (on mobile), go to Parental Controls, and choose Add Parent.

To access all parental controls, start by going to Settings, then Parental Controls, then Settings You Manage. You can then customize things like Content Maturity, Communication Controls and whether or not they can access private servers. You can also block a specific Roblox experience, even if it is rated for your child's age, by selecting Blocked Experiences.

Minecraft

Parental controls on Minecraft are done through your XBox Live account at <https://account.xbox.com/settings>. Select your child's gamer tag at top right and then:

- Select “Online Safety” to decide if your child can join mutiplayergames or access Minecraft realms, as well as whether they can add or remove friends
- Select “Privacy” to decide who can chat with your child. Choose “Friends” if you want them to be able to chat with their XBox Live friends and “Block” if you don’t want them to chat with anyone through Minecraft.

SOCIAL NETWORKS

Most social networks have Parent or Family centres. If you want information about one that’s not listed below, do a search for the social network’s name and “parent centre” or “family centre.”

TikTok

Make sure your teen gives their accurate age when registering: teens aged 13-15 start with safer default privacy settings.

TikTok offers a Restricted Mode that “limits the appearance of content that may not be appropriate for all audiences.” To turn it on, choose “Digital Wellbeing” in the settings, tap “Turn On,” set a passcode and toggle “Restricted Mode” to On.

You can also use Family Pairing to link your child’s account to yours and manage it. Tap Profile, then Menu, then Settings and Privacy. Tap Family Pairing and then Continue, tap Parent or Teen, and then Next to link the accounts. After that, you can view and control your teen’s settings by tapping Family Pairing.

Snapchat

To set up parental controls on Snapchat, search for your teen’s username and add them as a friend. Once they’ve accepted your friend request, tap the gear icon at the top right corner of your profile page and choose Family Center. Choose your teen’s account and send an invitation. Once they’ve accepted, you can use Family Center to set content controls and review their contacts.

Instagram

Make sure your teen gives their accurate age when registering: teens aged 13-15 need parental permission to change their privacy settings and cannot livestream.

To make a supervised account, go to the Family Center (<https://familycenter.meta.com/ca/our-products/instagram/>) and choose Create Invitation. Once they’ve accepted the invitation, you can set time limits, see who they follow and who follows them, and see who they have chats with (though not the content of those chats.)

MONITORING SERVICES

Some commercial products and services allow you to directly monitor what your children are doing online, as well as to block different kinds of content. While these can be useful with young children, and may be an appropriate consequence if your kids have misused digital tools, it's important to keep in mind that they are only ever part of the solution. Kids are very good at getting around tools like these and using these tools can lead children to try to cover up when things go wrong, rather than coming to you for help. If you do decide to use monitoring software because you are concerned about your child's safety, it's important you be upfront about it rather than spying behind their back as this will erode trust.

FINAL TIPS

Most of these settings can be changed by your kids if they know how: the most secure are the operating system settings, which you can require a password to change.

Remember that you are the most effective parental control. No technical tools are perfect, and they should never be a substitute for talking to your kids about what is and isn't appropriate and how you expect them to behave online.

When kids are exposed to inappropriate content, it's often by accident – and kids say that's one of the things that bothers them the most. Make sure you've told your kids to come and tell you if they ever see something, and reassure them that they won't get in trouble if they do.