CYBER AND FRAUD HUB

Keeping Children Safe Online

A Guide for Parents, Carers, and Guardians

cyberfraudhub.org

Keeping Children Safe Online.

The internet, social media, video sharing platforms, and instant messaging apps hold a great attraction for children and can, if used safely, be of great social and educational benefit.

Unfortunately, these resources can also create a less-than-positive environment where children, through no fault of their own, may find themselves targeted by online bullies or more serious predators.

This guide aims to provide advice to parents, grandparents, carers, guardians, siblings, and children themselves, highlighting key things to look out for to stay safe online.

Contents:

General Warnings

- Everyone should be vigilant about who they interact with online. Sometimes, people disguise their profiles and pretend to be other children, so caution is advised regarding the information users share with each other.
- Children should be advised not to share information such as full names, pictures of themselves, where they live or what school they attend.
- When filming videos or taking pictures of themselves, children should be cautious of any revealing information in the background before sharing. For example, TikTok haul videos may unintentionally show addresses, reveal their school uniform, or display pictures of their house, which could be identifiable.
- A popular trend online - especially on TikTok - is lifehacks. While many of these are harmless, there has been a rise in potentially dangerous lifehacks being shared without proper warnings. These might include activities like mixing chemicals unsafely or testing durability by dropping mobile phones.

Cyberbullying

- Cyberbullying is common online and can have a severe impact on mental health. Parents should check in with their children regularly in case they experience any abuse online. If it does occur, users should block the offending person and set their account to private, if it isn't already. Everything that is said should be documented then reported to the platform it is taking place on. If the child knows the person bullying them in real life, the bully can also be reported to the school, and in serious cases, the police.
- Cyberbullying often takes the form of direct messages and posts targeting an individual. However, it can also involve indirect taunting online, including behaviours such as spreading images, abusive public comments, and sharing private messages.

Conversations to have:

Internet Trends

An internet trend is something that becomes popular online, such as the ALS Ice Bucket Challenge in 2014. While some trends can be simple and positive, others can be dangerous, like the Salt and Ice Challenge, where people applied ice and salt to their skin, causing burns that could result in permanent damage. It is important to talk to children about how not everything they see online is a good or safe idea.

Oversharing

Video games with online capability often have text chat or voice chat. If your kids play online games, it's important they understand the difference between what they can safely discuss with strangers versus what they can share with friends they truly know.

Do not give out:

- Home address
- Phone number
- Full name
- Age
- Which school they attend or anything unique to where they live

Giving out too much information can lead to people online finding out too much about their life or even stalking them. This is also important to remember while talking to 'online friends'.

Grooming

A groomer is an extremely dangerous individual who uses technology such as the internet, to build a relationship with a young person, with the intention of tricking, pressuring or forcing them into doing something sexual, like sending images or videos of themselves. Online, it is easier for people with these intentions to pretend to be someone they're not, like a friend, mentor, boyfriend or girlfriend.

A groomer does not look a certain way, they can be any age and any gender.

The signs to look out for:

- **They ask to keep conversations private.**
- **They try to find out personal information.**
- **They send lots of messages.**
- **They give lots of compliments about your child's physical appearance.**
- **They give compliments about how mature your child is.**

It is important to know who your children are talking to online, but you can only monitor so much. It is much more important that they know and understand the dangers themselves, and you are a safe space to discuss any worries.

Video Games Age Ratings

Some games contain inappropriate content for children. This can include graphic violence and also profanity, drugs, and sexual content. However, in the online age there is a darker side. If you buy an 18-rated online game, your child is going to be playing with people who are (mostly) 18 or older. This means adults will talk like they are with other adults. Your child may hear profanities or pick up language which may not be appropriate.

Sextortion

Sextortion is a growing type of cybercrime that is used by multiple crime groups. In this type of crime, the offender poses as someone they are not and attempts to manipulate the victim into sending nude or semi-nude photos of themselves. It will usually start with the victim being contacted by someone they don't know on social media. After a short conversation, the offender often moves the discussion to an encrypted messaging app. They then request images from the victim, sometimes sending samples themselves.

Once the images are sent to the offender, they will use them to threaten the victim and attempt to extort the victim out of money or to reveal information (such as a home address) or get them to complete a certain action.

These types of attack can lead to devastating effects on the victim such as:

- **Financial loss.**
- **Physical or sexual abuse.**
- **Bullying.**
- **Trauma and depression.**
- **Suicide.**

Prevention

- **Increase the privacy settings on your child's social media accounts to prevent anyone they don't know from contacting them or accessing the content they post.**
- **Discuss what sextortion is and what the leading factors and signs are.**
- **Make them aware that you are a safe place and that they can and should talk to you if any suspicions or worries arise.**
- **Reassure children that this issue can be resolved, and they should not worry.**
- **If they are a victim of a sextortion scam, you should immediately call Police Scotland.**

More information about sextortion and the support available can be found on the Police Scotland website at: https://www.scotland.police.uk/advice-and-information/internet-safety/sextortion/

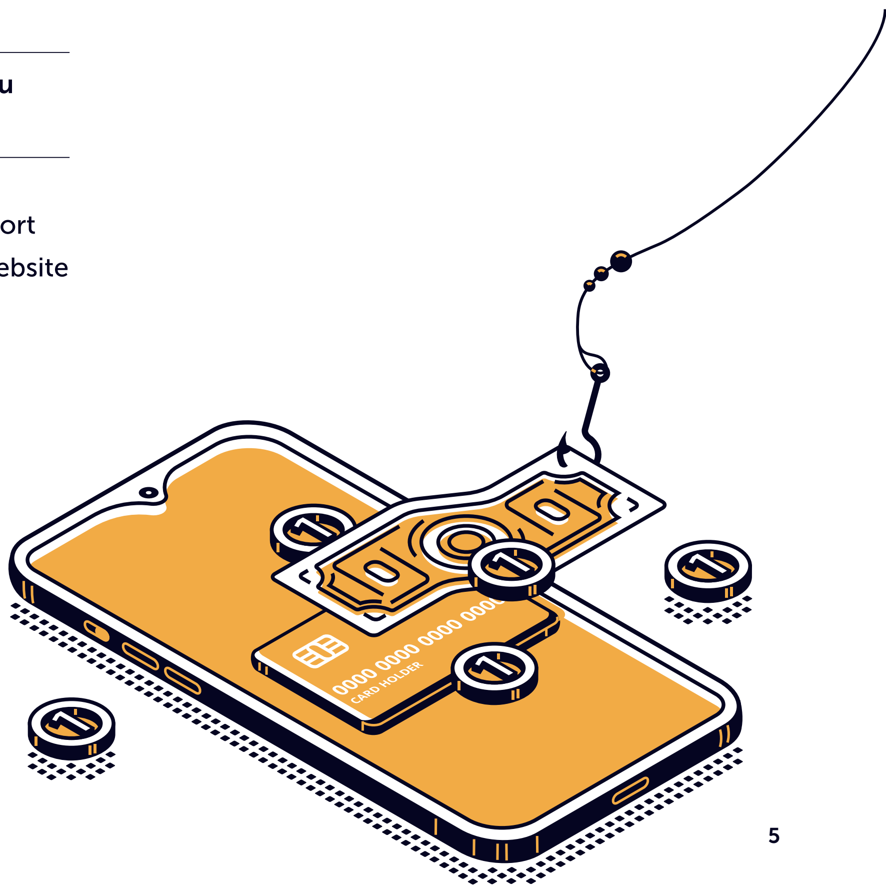
Scams and Phishing

Scams and phishing are attempts from cyber criminals and malicious users on the internet to steal money and information. These can come through various communication methods:

- **SMS.**
- **Email.**
- **Social media posts and messages.**

A common method these scammers use on young people is to create a fake account of a celebrity that is popular amongst young people, such as a YouTuber or Twitch streamer. They will usually ask the victim to buy Amazon and PayPal gift cards and send them to the scammer, usually in return for a prize, such as an expensive phone or game console. Some influencers do legitimate giveaways, but scammers use this to their advantage.

It is important to tell your child that these scammers exist. Make them aware that if they find themselves in a situation like this, to come and talk to you – you are a safe space.



Exploitation by Organised Crime Groups

Criminal groups have been known to exploit young people to achieve their goals. The groups do this by encouraging children to allow them to use their bank accounts to transfer funds for money laundering, often by saying that they themselves don't have a bank account and need to transfer money to a friend, or family member in another part or the UK or worldwide.

In return for this, children are rewarded with items such as new trainers, clothing or online gaming vouchers.

This type of activity is illegal and could lead to the involvement of the police.

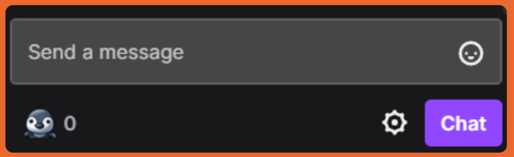
It is important to discuss these dangers with your child. If they are contacted by someone to perform illegal favours and actions, encourage them to speak with you. It is important to contact the police. This activity could be linked to criminal gangs responsible for drug, arms and people trafficking.

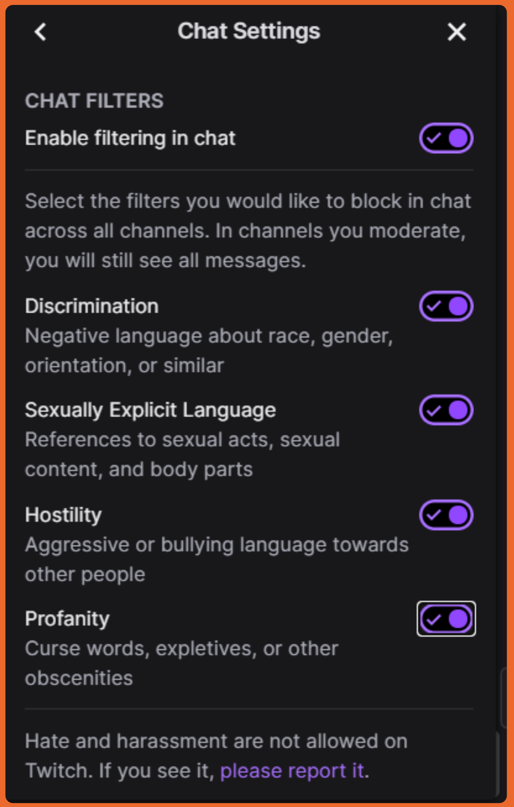
Video Games

Twitch

Twitch is an online streaming service associated with (but not limited to) gaming. This means a 'streamer' can play a game and be watched by hundreds or thousands of people live.

As a viewer, if you have an account you can talk in a chat box which can be read by anyone watching the stream, and the streamer themselves. There are typically moderators for larger streams, watching out for anything that goes against the stream's rules. There is an option to enable chat filtering for profanity and other topics. Enabling this is a good idea for younger viewers.




Chat Settings

CHAT FILTERS

Enable filtering in chat ☑

Select the filters you would like to block in chat across all channels. In channels you moderate, you will still see all messages.

Discrimination ☑
Negative language about race, gender, orientation, or similar

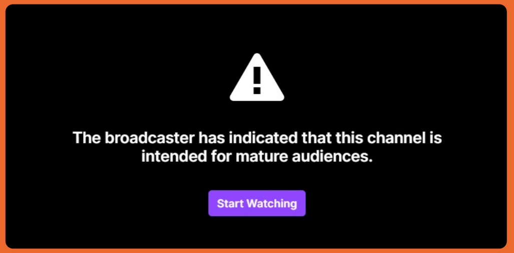
Sexually Explicit Language ☑
References to sexual acts, sexual content, and body parts

Hostility ☑
Aggressive or bullying language towards other people

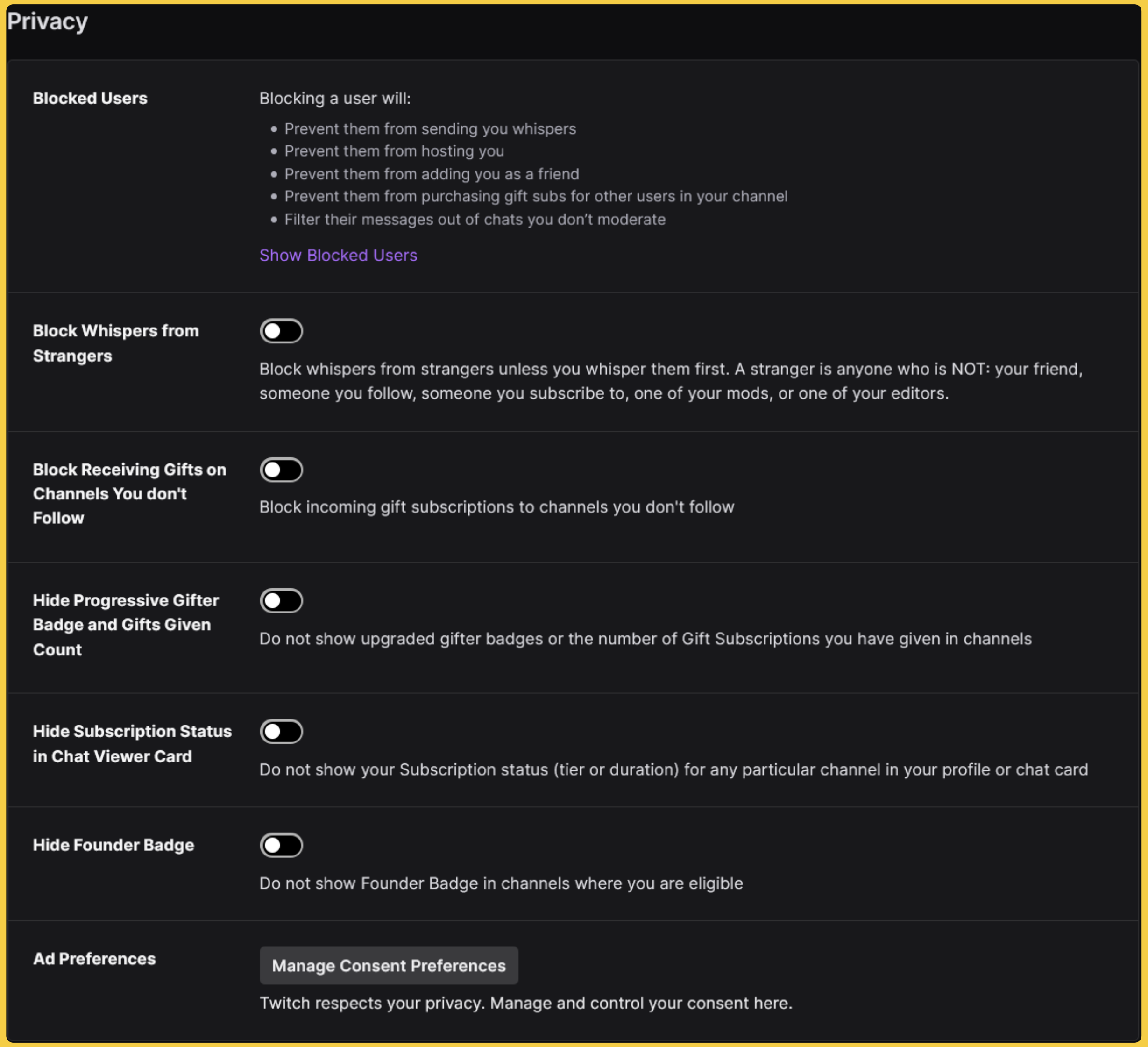
Profanity ☑
Curse words, expletives, or other obscenities

Hate and harassment are not allowed on Twitch. If you see it, please report it.

Twitch has a large variety of streamers aimed at a range of audiences. If the game they are watching has an age rating of 16/18 it is likely the stream is aimed at an older audience. Twitch streamers sometimes include a warning about how the stream is intended for 'mature audiences'. This warning is easy to click past; make sure to check if the streamer is appropriate for your child.


The broadcaster has indicated that this channel is intended for mature audiences.

There are several options for privacy. Users can block other users. They can also block private messages (called 'whispers' on Twitch) from strangers.


Privacy

Blocked Users

Blocking a user will:
- Prevent them from sending you whispers
- Prevent them from hosting you
- Prevent them from adding you as a friend
- Prevent them from purchasing gift subs for other users in your channel
- Filter their messages out of chats you don't moderate

Show Blocked Users

Block Whispers from Strangers ○

Block whispers from strangers unless you whisper them first. A stranger is anyone who is NOT: your friend, someone you follow, someone you subscribe to, one of your mods, or one of your editors.

Block Receiving Gifts on Channels You don't Follow ○

Block incoming gift subscriptions to channels you don't follow

Hide Progressive Gifter Badge and Gifts Given Count ○

Do not show upgraded gifter badges or the number of Gift Subscriptions you have given in channels

Hide Subscription Status in Chat Viewer Card ○

Do not show your Subscription status (tier or duration) for any particular channel in your profile or chat card

Hide Founder Badge ○

Do not show Founder Badge in channels where you are eligible

Ad Preferences

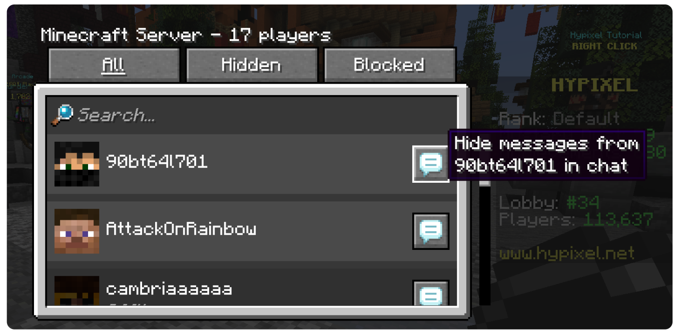
Manage Consent Preferences

Twitch respects your privacy. Manage and control your consent here.

Viewers of streams can also pay for 'bits' and pay to be a 'subscriber'. These support the streamer to keep doing what they are doing. They can give the viewer special perks such as their messages being highlighted in a chat or special 'emotes' (like emojis). Viewers do not need to do this.

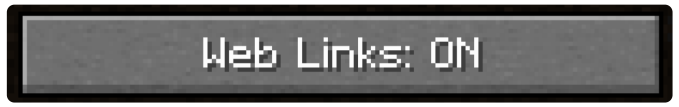
Minecraft

On Minecraft (Java edition), there is a multiplayer option. By joining a 'server', someone can play with many users. Once playing, they can press the 'P' key. This allows users to hide messages from certain players. It also allows users to block others.

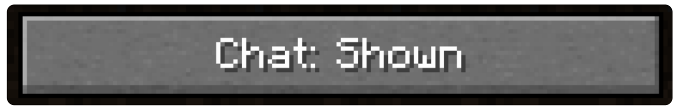

Minecraft Server - 17 players

Hide messages from 90bt64l701 in chat

Users can send links in a chat. You can stop a child accidentally clicking on a link in the chat by turning web links off.


Web Links: ON

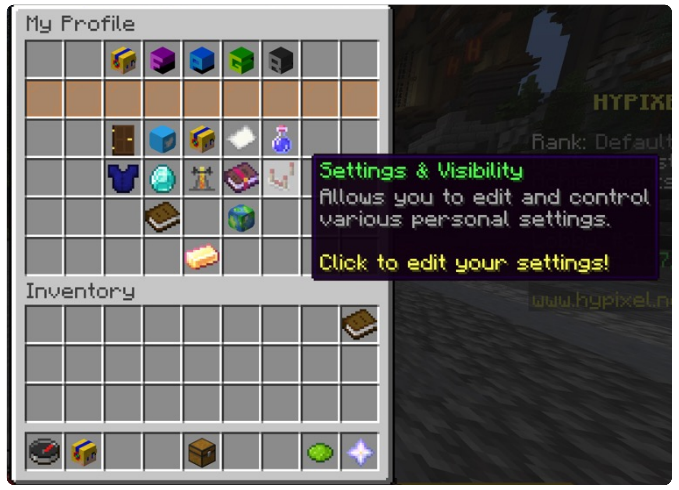
Users talk to each other in the chat. Some servers have completely unmoderated chat. The chat can be removed from the screen. This will mean the user will not be able to see what others are saying and will also stop them from chatting themselves. This could however stop some of the games your child tries to play from working.


Chat: Shown

Hypixel

The most popular server on Minecraft is called Hypixel. On Hypixel players can play a wide range of games like Pictionary and Hide and Seek with others. Hypixel has a lot of functionality which can be changed.

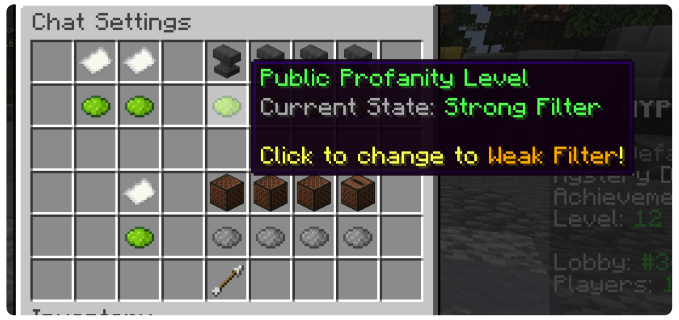
After joining the Hypixel server, there is a player head in the hotbar at the bottom of the screen. By right-clicking while holding it, a menu is opened.



Settings & Visibility
Allows you to edit and control various personal settings.
Click to edit your settings!

By clicking on 'Settings & Visibility' there are many options which can be changed.

By clicking on the 'Chat Settings' option, the visibility of chat can be enabled and disabled, and profanity levels are available for different groups of players.



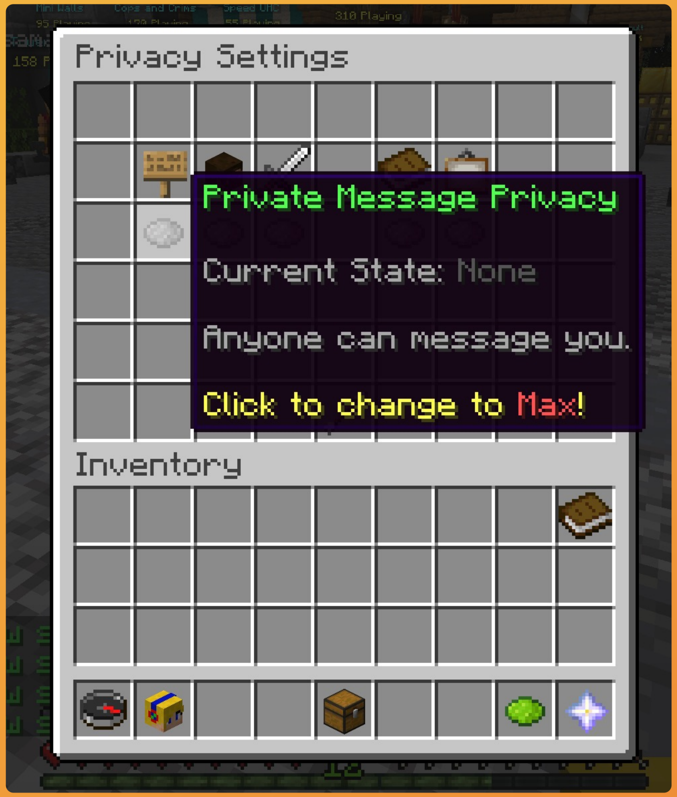
Public Profanity Level
Current State: Strong Filter
Click to change to Weak Filter!

By clicking on 'Privacy Settings', users can change their privacy settings. There are privacy settings for:

- **Private messages.**
- **Friend request.**
- **Duel invite.**
- **Party invite.**
- **Guild invite.**

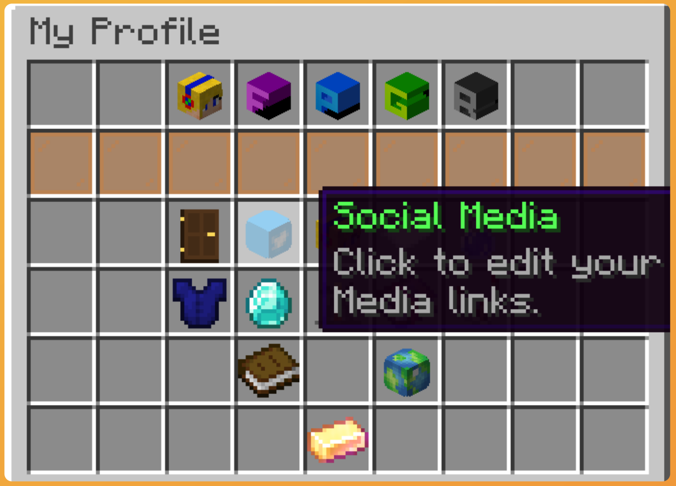
For example, private message settings can be set to:

- **Anyone can message you.**
- **Staff, friends, guild members, and party members can message you.**
- **Staff, friends, and guild members can message you.**
- **Staff and friends can message you.**
- **Only staff can message you.**



Private Message Privacy
Current State: None
Anyone can message you.
Click to change to Max!

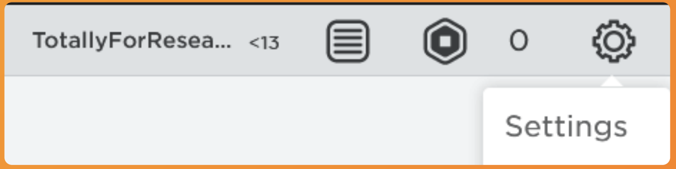
It is also possible to link social media accounts, including Twitter, Discord, YouTube, Instagram, and others. Once added, anyone can see information about your child from their social media feed.
It is recommended not to enable this feature.



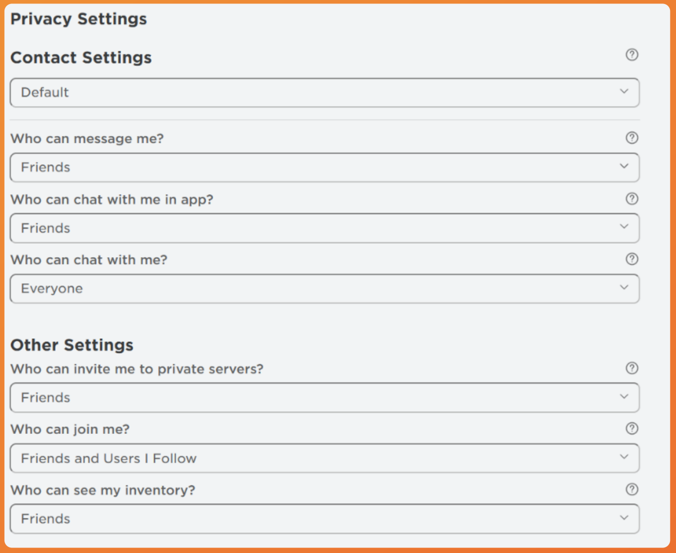
Social Media
Click to edit your Media links.

Roblox

Roblox allows for users to join servers, to play with others. It is popular on mobile devices, PC and Xbox. Roblox allows for a range of parental controls. These options can be secured with a pin, ensuring that your child cannot change them.



Privacy settings can be adjusted so that only certain users can message your child, and only certain users can invite your child to play with them.


Privacy Settings

Contact Settings
Default

Who can message me?
Friends

Who can chat with me in app?
Friends

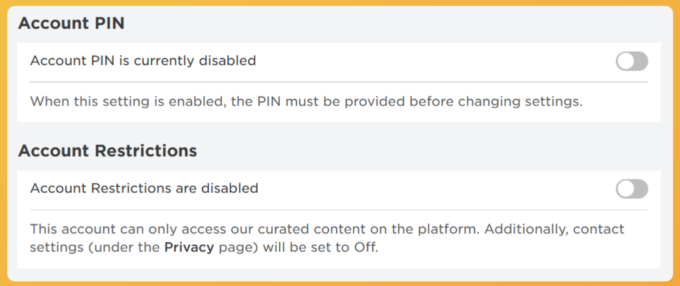
Who can chat with me?
Everyone

Other Settings
Who can invite me to private servers?
Friends

Who can join me?
Friends and Users I Follow

Who can see my inventory?
Friends

Account restrictions can be turned on so the content they can access is age - appropriate, and the chat will be disabled.



Account PIN

Account PIN is currently disabled

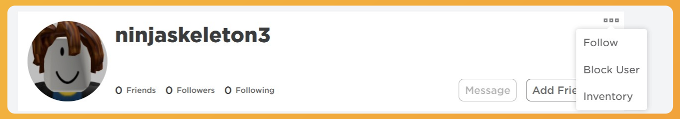
When this setting is enabled, the PIN must be provided before changing settings.

Account Restrictions

Account Restrictions are disabled

This account can only access our curated content on the platform. Additionally, contact settings (under the **Privacy** page) will be set to Off.

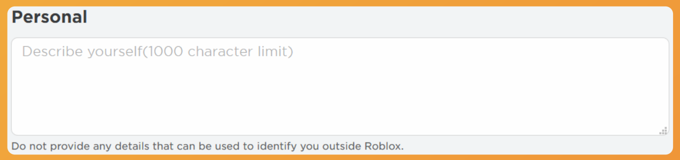
Users can be blocked by going to their page.



ninjaskeleton3

0 Friends 0 Followers 0 Following

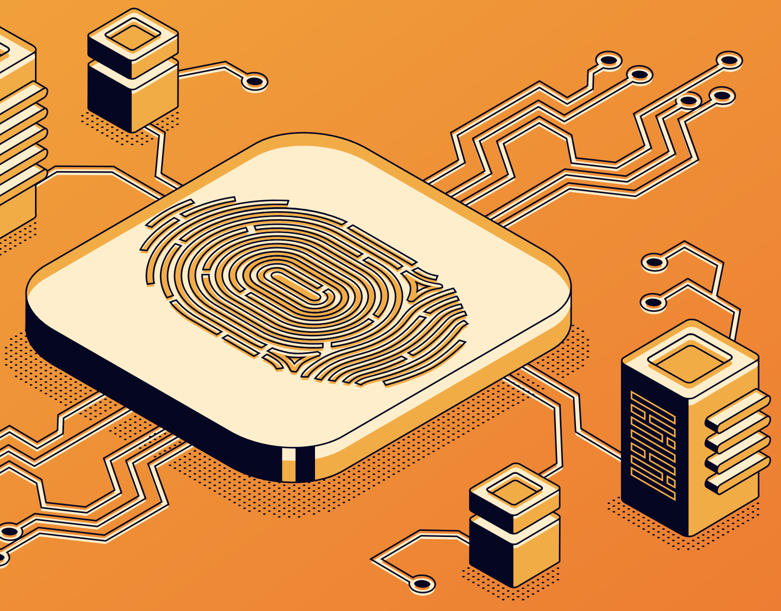
Parents should keep an eye on what information their child adds to the personal bio section. It is never a good idea to include anything identifiable such as a real name, image, information about where they live or what school they attend.



Personal

Describe yourself(1000 character limit)

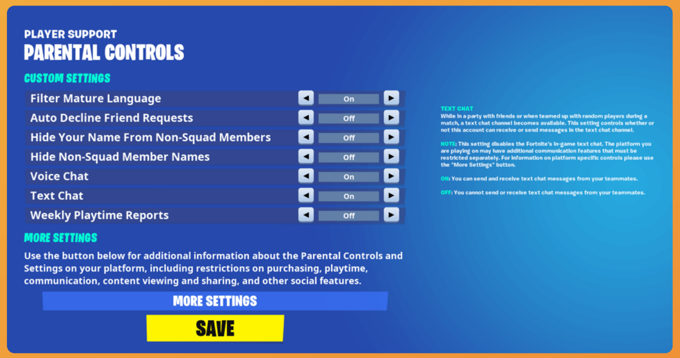
Do not provide any details that can be used to identify you outside Roblox.



Fortnite: Battle Royale

Fortnite is an online game where the aim is to stay alive, whilst eradicating the other players/teams/ monsters. The game is violent, but it is not gory.

There are parental controls within Fortnite, and a pin can be added to stop your child changing them.



PLAYER SUPPORT

PARENTAL CONTROLS

CUSTOM SETTINGS

Filter Mature Language	On
Auto Decline Friend Requests	Off
Hide Your Name From Non-Squad Members	Off
Hide Non-Squad Member Names	Off
Voice Chat	On
Text Chat	On
Weekly Playtime Reports	Off

MORE SETTINGS

Use the button below for additional information about the Parental Controls and Settings on your platform, including restrictions on purchasing, playtime, communication, content viewing and sharing, and other social features.

TEXT CHAT

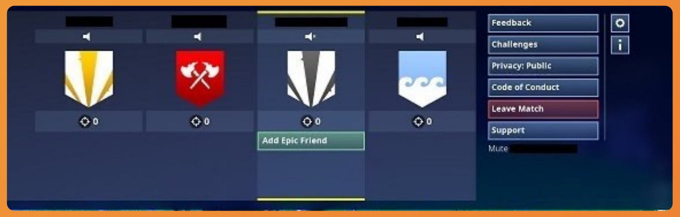
While in a party with friends or when teamed up with random players during a match, a text chat channel becomes available. This setting controls whether or not this account can receive or send messages in the text chat channel.

NOTE: This setting disables the Fortnite's in-game text chat. The platform you are playing on may have additional communication features that must be restricted separately. For information on platform specific controls please use the "More Settings" button.

ON: You can send and receive text chat messages from your teammates.

OFF: You cannot send or receive text chat messages from your teammates.

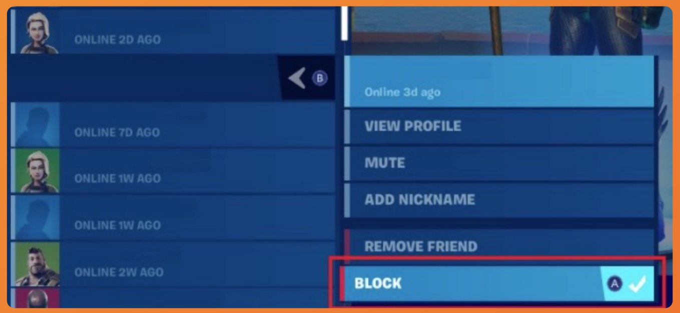
In the menu (accessed by pressing 'Escape' or 'Pause' on consoles) players can also be muted by clicking on their player card and then clicking the 'Mute' button. On some devices you only need to click on the player card.



[redacted] [redacted] [redacted] [redacted]

Mute [redacted]

Players can also be blocked in the social tab.



Social Media

Snapchat

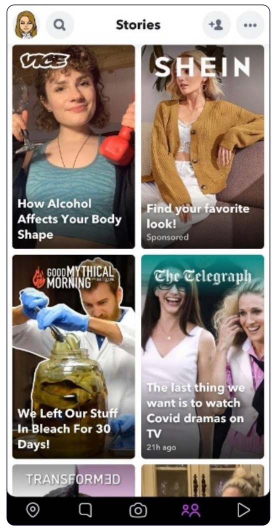
Snapchat is a mobile messaging app. Users can send photos and videos (Snaps) to their friends. The app's main feature is that pictures and messages can only be viewed for a short time before they are deleted and can no longer be accessed by the receiver.

Features

- 'SnapMaps' is a Snapchat feature where users can share their location real-time with their friends and see other users who have the same feature enabled. This feature can be dangerous - it relies on the friends list being trusted people only, and those friends having secure accounts. It is possible to disable sharing your location by selecting 'Ghost Mode'.
- 'Discover' is a section of Snapchat that displays popular articles from various media channels. These can sometimes contain explicit content that is not appropriate for children.
- 'Stories' are spaces where multiple Snapchats can be added that can be viewed for 24-hours. Users can also create 'Private Stories' where they can select which friends can view a story. It is possible for users to block other users from viewing their story by going to Settings>View My Story>Custom.
- 'Quick Add' shows friends of friends that users may know and want to add. This allows users to see your username and attempt to add you. This can be turned off in Settings>See Me in Quick Add.

Harm Prevention

- Due to the nature of disappearing messages, pictures, and videos, Snapchat can be difficult to monitor when it comes to protecting your child. Bullying can also be hard to detect. Make sure to have a conversation with your child to discuss the risks of using the platform and let them know they should save any harmful messages in the chat or screenshot any hurtful pictures to discuss what to do about it, with you.
- The age restriction on Snapchat is 13, and during the sign-up process, users are asked for a date of birth to ensure the user meets the age restriction. Children may, however, go around this by entering a fake birthday. If a user enters in a birthday younger than 13, they are directed to a child-restricted version of snapchat called 'SnapKidz'. This version does not allow users to add friends or share pictures/videos.
- Make sure to have a strong password and set up Two-Factor Authentication to protect your child's account.
- If your child is being bullied, harassed or has any kind of safety concern, it is possible to report a user. This can be done through Settings>I Have a Safety Concern, and this will show all information about how to report a Snap, Story or account.



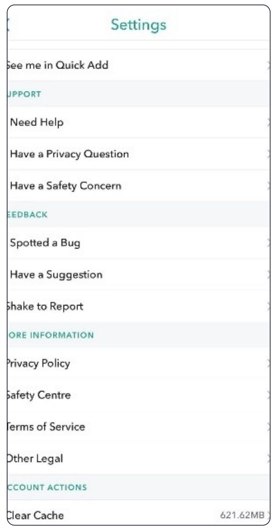
Stories

How Alcohol Affects Your Body Shape

Find your favorite look!
Sponsored

We Left Our Stuff In Bleach For 30 Days!

The last thing we want is to watch Covid dramas on TV
21h ago



Settings

ee me in Quick Add

UPPORT

Need Help

Have a Privacy Question

Have a Safety Concern

EEDBACK

Spotted a Bug

Have a Suggestion

hake to Report

ORE INFORMATION

rivacy Policy

afety Centre

erms of Service

ther Legal

CCOUNT ACTIONS

lear Cache 621.62MB

TikTok

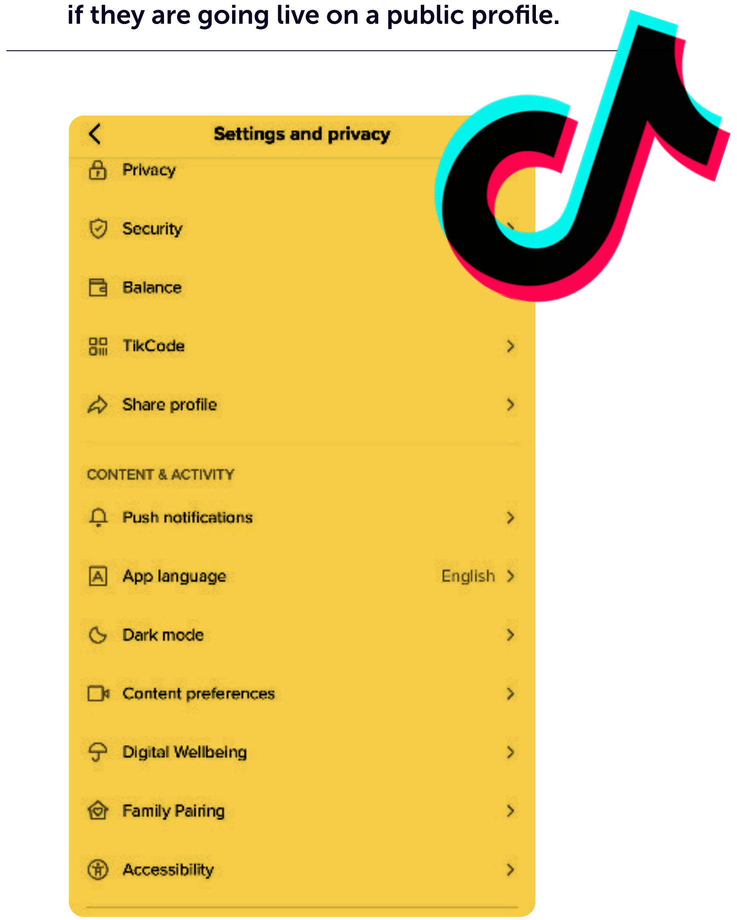
TikTok is a social networking app that shares videos made by other users. These videos range from a variety of genres such as comedy, dance and education. The length of the videos can be anything from 3 seconds to 1 minute. It was originally aimed at children; however, the platform has grown massively and now caters to all ages.

Features

- The 'For You' page is curated by an algorithm that generates and displays content tailored to the user's interests. Videos that are shown are selected based on the user's viewing habits, prioritising popular content similar to what they have already viewed and liked.
- The 'Following' page will display videos belonging to accounts that the user follows.
- Users can create 'Duet' videos, in which they can post side-by-side with a video from another creator on TikTok. There is also an option for users to 'Stitch' videos. This collaborative feature allows users to integrate a clip from another video into their own content. By selecting and trimming a segment of an existing video, they can add their own creative response or continuation.
- Users can also Direct Message on TikTok and share TikToks with one another.
- Live streaming allows for users to video themselves live, and have people watch real-time and comment/interact with the user.

Harm Prevention

- The age restriction on TikTok is 13, however there are ways around this for younger children to create accounts. Accounts found to belong to users under 13 are typically banned or reported. If the user of the account is between 13-15 years old, their accounts are automatically set to private, meaning only friends can comment and other users are restricted from using features like Duet, Stitch or downloading videos.
- A strong password is essential and TikTok now offers Two-Factor Authentication, security alerts for suspicious activity, and the option for users to view what devices their account is logged into.
- The 'Privacy' section in settings offers various options to make a user's account more secure, including blocking direct messages, applying comment filters and controlling who can view a user's liked videos.
- 'Family Pairing' is a good feature if a parent would like to monitor what content their child views, track their watch time and change their child's account to private. This is in Settings>Family Pairing. It is done easily by linking the accounts together with a QR code.
- The age limit for live streaming is 16. However, teens should be mindful not to reveal private information, such as their location or school, if they are going live on a public profile.



Settings and privacy

Privacy

Security

Balance

TikCode

Share profile

CONTENT & ACTIVITY

Push notifications

App language English

Dark mode

Content preferences

Digital Wellbeing

Family Pairing

Accessibility

Instagram

Instagram is a photo-sharing social media platform. Users can post photos and videos onto their profile, share stories, and send direct messages.

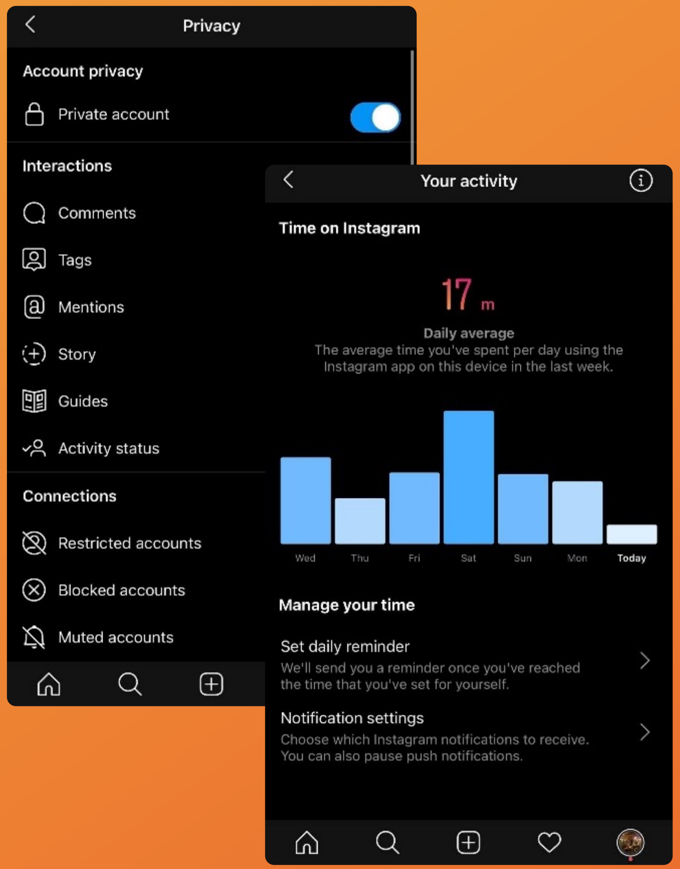
Features

- 'Stories' are images or videos that a user can upload, which disappear after 24-hours. Others can like, comment, or react to the story but only the poster will be notified. Stories can be viewed by anyone if a user's profile is public.
- 'Reels' are similar to TikTok videos. Users can record themselves and add music or effects to short clips, typically ranging from 15 to 90 seconds.
- Instagram also has a 'Disappearing Messages' feature that allows for pictures/videos to be sent that can only be viewed once and then delete.
- IGTV (Instagram TV) allows users to post longer videos on Instagram. These videos can appear in the main feed or in the IGTV section. They may also be discovered through the 'Explore' feed, where users can see content from accounts they don't follow.
- Users can also livestream themselves in real-time and have their followers watch them and interact through commenting or going live with them (like a public facetime).

Harm Prevention

- In the Instagram terms of service, the age restriction is 13 years old, however there's no process to verify this. Therefore, many children have Instagram. Teens under 16 automatically have their accounts set to private.
- The content that is displayed on Instagram depends on who the user follows. There is no way to restrict who a user may follow, meaning it is easy for a child/teen to see explicit content and posts about concerning topics. Adverts are also displayed which cannot be controlled, and are tailored to the user's online activity, so it is possible for explicit adverts to be displayed.
- Set up Two-Factor Authentication on Instagram by going to Settings>Security>Two-Factor Authentication.
- Children/teens may want to consider putting their accounts on private for their own personal safety, especially if they post pictures with sensitive information such as where they live, go to school or their daily routine.
- Comment Controls can be placed on an account to restrict who can comment on a post, and to block comments with specific words.

Users can disable the 'Resharing' feature to prevent others from sharing their stories. Users can set a time limit on how long they are spending on the app by going to Settings>Your Activity>Set Daily Reminder. This feature only alerts users when they have reached their set time limit; it doesn't enforce the limit.



Privacy

Account privacy

Private account

Interactions

Comments

Tags

Mentions

Story

Guides

Activity status

Connections

Restricted accounts

Blocked accounts

Muted accounts

Your activity

Time on Instagram

17 m

Daily average

The average time you've spent per day using the Instagram app on this device in the last week.

Manage your time

Set daily reminder

We'll send you a reminder once you've reached the time that you've set for yourself.

Notification settings

Choose which Instagram notifications to receive. You can also pause push notifications.

Facebook

Facebook is a social media platform where users can share photos, videos and status updates with their friends. Each user has a profile that can display personal information such as their name, place of study, and hometown. Privacy settings on Facebook are highly customisable, allowing users to control who sees their content. Messenger is the messaging app connected to Facebook; however, it is now its own independent platform, and a Facebook profile is no longer required to use it.

Harm Prevention

- **Set up Two-Factor Authentication on Facebook by going to Settings>Security and Login> Use Two Factor Authentication.**
- **The content displayed on Facebook is dependent on who the user is friends with. It is advised that young people only add people they know and trust. A lot of explicit and unsafe content can be shared on Facebook, but this will depend on what a user's friends share, and the pages they follow.**
- **A lot of sensitive information can be shown on a user's Facebook profile, including family members, place of birth, current location, job details and education history. To protect privacy, it is advised to restrict access to this information. These settings can be modified by going to Settings>Privacy>Manage your Profile / Your activity / How People Can Find and Contact You.**

X / Twitter

X, previously known as Twitter, is another social media platform, where users post short updates called 'Tweets.' These are similar to Facebook status updates but are limited to 280 characters. The content that appears on a user's feed depends largely on who they follow. However, many child-friendly content creators do not maintain child-friendly pages on X, which may expose younger users to inappropriate material.

Harm Prevention

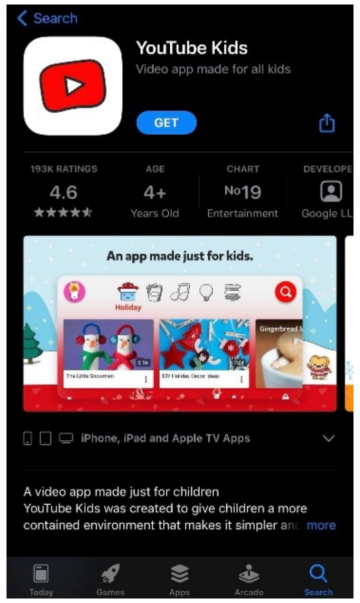
- **Set up Two-Factor Authentication by going to Settings and Privacy>Security and account access>Security>Two-Factor Authentication.**
- **Set the profile to 'Private', this is especially important if any Tweets made reveal any personal information. This can be done by going to Settings and Privacy>Privacy and Safety>Audience and Tagging > Protect your Posts.**
- **X has a feature where users can tag their location in their Tweets. Children and teenagers should avoid using this feature for their safety, especially if their profile is public.**

YouTube

YouTube is an online video sharing platform with a wide range of content, including vloggers, gamers, educational videos and more. Anyone can upload videos, and similarly anyone can watch public videos. There can be lots of inappropriate content on YouTube for children, however there are many ways to control access.

Harm Prevention

- **YouTube offers a separate app called YouTube Kids, which features pre-filtered content suitable for children. It includes many parental controls, such as limiting screen time, adjusting volume, and managing the search function.**
- **Check which channels your children are subscribed to and encourage them to stick to these creators. This could prevent children from searching through YouTube for content and potentially coming across inappropriate videos. Notifications for new videos from subscriptions can be turned on to keep children engaged with safe content.**
- **If your child is uploading videos to YouTube, ensure they do not share personal information such as their home address, school, or phone number. Review their videos before they are uploaded or set them to private or unlisted (only accessible to people with a direct link).**



YouTube Kids

Video app made for all kids

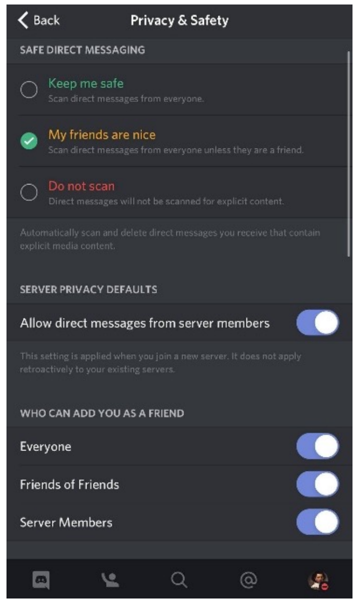
A video app made just for children
YouTube Kids was created to give children a more contained environment that makes it simpler an

Discord

Discord is a platform for voice chat and instant messaging. Servers can be created to host multiple people. Sometimes Discord servers are public for certain games, and anyone can join. These are sometimes heavily moderated to ensure safety, however users should be vigilant of who they are speaking to and what information they share.

Harm Prevention

- **The age restriction on Discord is 13 years old, however this is not verified anywhere. Some servers are created for younger audiences, however, there may be adults on the platform.**
- **To prevent children from receiving inappropriate direct messages, there is a feature that can be turned on that will scan direct messages for harmful content. This can be activated by going to Your Profile>Privacy and Safety> and selecting either 'Keep me safe', or 'My friends are nice'.**
- **It is also possible to restrict who can direct message you by going to Your Profile>Privacy and Safety>Server Privacy Defaults / Who Can Add You as a Friend.**
- **Users can create their own Discord servers. This is probably the safest way for children to interact, especially if they already have friends who they talk with online.**



Privacy & Safety

SAFE DIRECT MESSAGING

○ Keep me safe
Scan direct messages from everyone.

● My friends are nice
Scan direct messages from everyone unless they are a friend.

○ Do not scan
Direct messages will not be scanned for explicit content.

Automatically scan and delete direct messages you receive that contain explicit media content.

SERVER PRIVACY DEFAULTS

Allow direct messages from server members ●

This setting is applied when you join a new server. It does not apply retroactively to your existing servers.

WHO CAN ADD YOU AS A FRIEND

Everyone ●

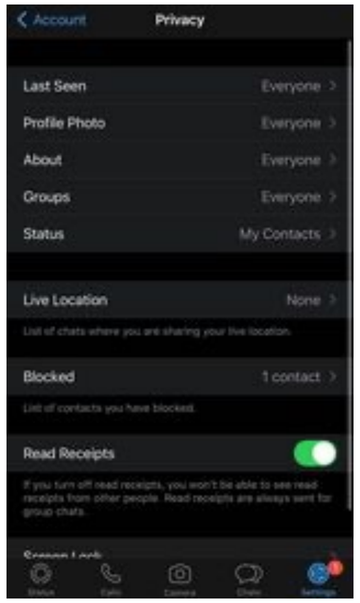
Friends of Friends ●

Server Members ●

WhatsApp

WhatsApp is a messaging application used to send text messages, voice notes, and make video or voice calls. It also allows for the sharing of images, videos and other downloadable files. It is used as an alternative to texting and many use it for group chats. WhatsApp uses phone numbers to connect users to one another.

Harm Prevention



< Account | Privacy

Last Seen: Everyone
Profile Photo: Everyone
About: Everyone
Groups: Everyone
Status: My Contacts

Live Location: None
List of chats where you are sharing your live location.

Blocked: 1 contact
List of contacts you have blocked.

Read Receipts: On
If you turn off read receipts, you won't be able to see read receipts from other people. Read receipts are always sent for group chats.

Screen Lock

- **The minimum age of use on WhatsApp is 16 years old; however, many people younger than this do have profiles.**
- **Due to WhatsApp using phone numbers for users to contact each other, it is a generally safe way for people to contact each other, as long as their number is not public. However, ensure that your child adjusts their settings so that only contacts can add them to groups and send messages. This can be done by going to Settings>Privacy>Groups.**

WhatsApp also has a default setting that automatically downloads media sent to a user. To prevent your child from downloading inappropriate photos, turn off this setting by going to Settings > Chats > Media Visibility. Live Location is a feature that allows users to share their current location. Make sure this is only activated with people you absolutely trust, and only when completely necessary.

Monkey

Monkey is a website that allows users to meet strangers online via video calls. This is done by randomly connecting users to others who are also online and linking the two profiles together. Although, Monkey is moderated 24/7 by a moderation team and uses AI to detect sexual content, it has been known to still have explicit and inappropriate content displayed by certain users. This content is visible to anyone that connects to this user on the platform.

The service is also accessible through a mobile app on the Google Play store, or on iPhone via a web browser.

Harm Prevention

- **The website does have an age rating of 18+ however, there is no age verification meaning an underage user could still access to the platform.**
- **The only 'security' option provided is the ability to delete the account from the platform.**

Threads

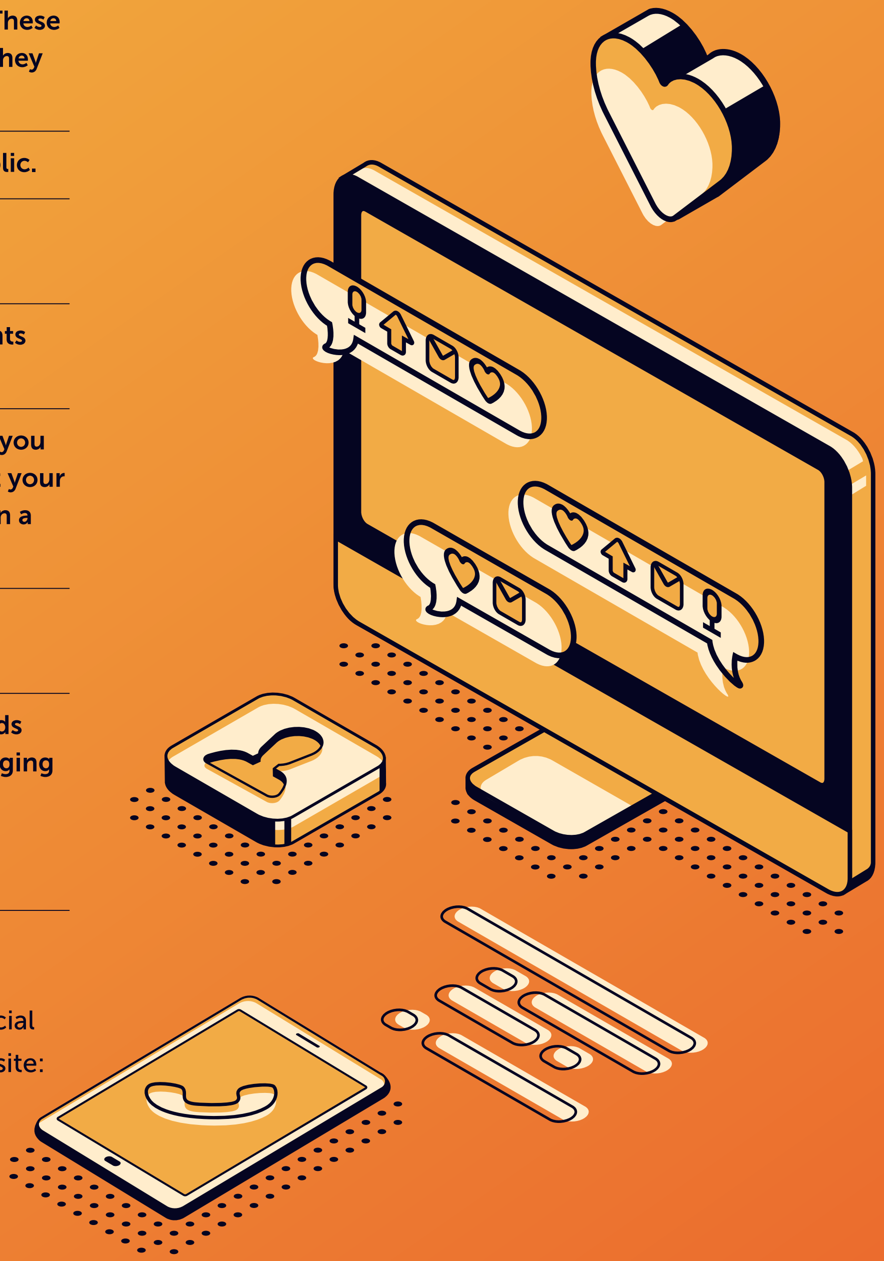
Threads is similar to X, but it is linked to an Instagram account. Users can write and post 'Threads', which are similar to posts on X. These posts have a character limit, but users can add additional posts if needed. Like other social media platforms, Threads may contain content that is inappropriate for children.

Prevention

- **Threads has the same age limit as Instagram (13 years), but there are no restrictions to using it if you have an Instagram account.**
- **The app has privacy settings that can be customised to add extra privacy controls. These can be found in Profile>Settings>Privacy. They include:**
    - **Privacy**: Set the profile to private or public.
    - **Mention parameters**: Control who can mention the account.
    - **Muted accounts**: Manage which accounts are removed from your child's feed.
    - **Hidden words**: These parameters allow you to define certain words you do not want your child to see. If those words are present in a post, then the post won't be displayed.
    - **Profiles you follow**: This shows which profiles your child follows.
    - **Suggesting posts on other apps**: Threads may display on certain other apps belonging to Meta. This will decide if the posts will display on other apps, these can't be activated if the account is private.

More resources

More resources about protecting yourself on social media can be found on the Police Scotland website: **https://www.scotland.police.uk/advice-and-information/internet-safety/social-media/**



Router Parental Controls

All routers supplied by your internet service provider (ISP) contain control panels. Within these control panels, accessed through your web browser, the settings of your home networks can be changed, such as the network name, password, and other basic settings. Alongside this, the privacy and security settings of the network can be configured. This includes adult filters, specific site blocking, keyword blocking, setting specific times that devices can access the internet. These filters can be set up on a per-device rule, or a general rule.

For your specific ISP and router, the relative links can be found within the subheadings of the ISP.

BT Group

Accessing the Admin Panel

Once you've accessed the admin panel, there are multiple options to both manage and view the network. This includes the option to change the network name, password, as well as viewing all the connected devices. This can be useful in case there is an unauthorised user. Alongside this, time windows can be set up for devices to access the internet, these can be set up on a per-device basis. For example, a games console can only access the internet within a certain timeframe.

https://www.bt.com/help/broadband/learn-about-broadband/learn-about-the-bt-hub-manager

Adding Parental Controls to the Router

To manage parental controls, within the BT Hub system, an add-on must be added to the account, through the MyBT portal. However, this is already included within BT, it just needs to be activated. Once the parental control filters have been activated, the filters will be activated within 2 hours. The management of these can be done within your MyBT account.

https://www.bt.com/help/broadband/manage-service/how-to-keep-your-family-safe-online-with-bt-parental-controls-an#settingup

Sky

Accessing the Admin Panel

Once you've accessed the admin panel, there are multiple options to both manage and view the network. This includes the option to change the network name or password, as well as viewing all the connected devices. This can be useful in case there is an unauthorised user. Additionally, you can set up time windows for devices to access the internet on a per-device basis. For example, a games console can only access the internet within a certain timeframe. For example, a games console can only access the internet within a certain timeframe.

https://helpforum.sky.com/t5/Broadband-Talk/Accessing-your-router-settings-page-192-168-0-1/ba-p/2649511

Virgin

https://www.virginmedia.com/help/virgin-media-configure-advanced-settings-on-your-hub

TalkTalk

https://community.talktalk.co.uk/t5/Articles/Change-your-router-admin-password/ta-p/2204673

Vodafone

https://modemly.com/Vodafone-Vodafone-Box-router-setup

Device Parental Controls

Apple

Within the Apple operating system (iOS), it is possible to implement parental controls on the device. These controls can be used to prevent app store purchases, restrict access to the Game Centre, and limit the web content that can be viewed.

To access these, go to the settings of the device, and tap on 'Screen Time', select continue and choose 'This is my child's device'. Once this is done, the parental controls will be accessible.

The controls present within iOS are:

- **Prevent iTunes & App Store purchases – this can be configured to allow downloads, but not in-app purchases, as well as the download of free apps.**
- **Allow built-in apps and features – This setting restricts the use of preloaded apps, such as Mail, Safari, Facetime.**
- **Prevent explicit content and content ratings – This setting can restrict the playback of explicit content, such as music videos, films, and TV.**
- **Prevent web content – This can be used to limit adult websites, or to create both a block list, as well as always allowed sites.**
- **Restrict Siri web search – Restricts Siri from searching the web and displaying explicit language.**
- **Restrict Game Centre – This can be used to restrict multiplayer games, adding friends and screen recordings.**
- **Allow changes to privacy settings - this setting restricts the general privacy settings of the device, choosing what information apps have access too.**

More information can be found here: https://support.apple.com/en-gb/HT201304

Android

Android devices, unlike Apple devices, have no parental control settings built into the system. However, there are parental controls available for the Google Play Store, and Google offers an application to enforce additional controls.

The Google Play parental controls can be set up by going into the settings of Google Play Store and navigating to Parental Controls. Once there, you can set up a PIN and choose the restriction level you would like to implement.

More information can be found here: https://support.google.com/googleplay/answer/1075738?hl=en-GB#zippy=

Google provides an application called 'Google Family Link'. Once this is installed on the child's device, it can be configured to monitor the child's activity, such as screen time, which can have a limit set to it.

More information can be found here: https://families.google.com/familylink/#

Windows

Windows have a Windows Family Safety option on their devices which allow you to keep track of a child's screen time and monitor their activity, including the games and software that they use, as well as how long they have used them for.

More information can be found here: https://www.microsoft.com/en-gb/microsoft-365/family-safety?ocid=family_signin

Parental Control Applications

Certain applications exist that allow you to have full access to what your child does on their phone. Some of the functionalities they offer are:

- **Monitor your child's text messages to prevent dangerous interactions.**
- **Make sure your child or teen doesn't receive calls from strangers or scammers.**
- **Always know the location of your child or teen.**
- **Track who your child or teen is talking to on social media and what personal information they could be sharing.**
- **Track which websites they visit.**
- **Set screen time limits or give access to certain applications only at certain times.**
- **Limit the apps they have access to.**

These applications typically come with a subscription fee, which can vary depending on the services and features provided. This can range from £3 to £5 a month.

Here are some examples of such applications:

mSpy: **https://mspy.mobi**
QuStudio: **https://www.qustodio.com/en/premium/**
Kids360: **https://kids360.app/**

While these applications can be useful for protecting your child or teen, it's still important to discuss the dangers of the online world with them.

Privacy Add-ons and Settings

Most modern browsers allow the use of extensions, which can range from tab managers to study aids. The extensions can also be used to upgrade the privacy and security of the browser, for example deleting malicious/tracking cookies and blocking ads. The use of these extensions allows for greater privacy while browsing the internet.

Here are some of the top-rated privacy extensions;

- **uBlock Origin – This extension blocks adverts within the browser, some of which contain trackers. These can track your browsing across web pages. uBlock Origin also blocks known malvertising (malicious advertising) domains, making the overall browsing experience more secure.**
- **Privacy Badger – This extension is built specifically to block scripts and trackers from browsers. After adding it to the browser you can see the number of trackers blocked by Privacy Badger.**
- **Disconnect Facebook – Facebook is known for its tracking of users around the internet and subsequent privacy issues. This add-on blocks Facebook from tracking you, even when you're not on the site.**

Another privacy focused change is using DuckDuckGo as your search engine. DuckDuckGo doesn't track your searches or use your data to display targeted ads, making it a more privacy-conscious choice.

Chrome

Chrome has some great extensions for both privacy and productivity. To access the Chrome Web Store, where you can add these extensions along with many other tools, visit the following URL:

https://chrome.google.com/webstore/category/extensions

Firefox

https://addons.mozilla.org/en-GB/firefox/extensions/

Safari

https://apps.apple.com/us/story/id1377753262

Mobile Providers Parental Controls

Mobile network and phone service providers offer the option to add parental controls to internet searches conducted via the SIM card. This can block any content that is marked as 18+ and prevent your child or teen from accessing it.

Three

The filter is turned on by default and can only be deactivated by verifying that you are over 18, by using a credit card. This can be found in the plan settings.

More information: https://www.three.co.uk/support/internet-and-apps/accessing-and-blocking-adult-content

EE

This mobile network provider has three variations of parental filters and control:

- **Moderate: This is the default setting. The user has access to social media but not the 18-rated content.**
- **Strict: The recommended setting for children under 13. Google searches will not show websites with adult content.**
- **Off: Gives user full access to the internet including 18-rated content.**

To access content in the 'Off' setting, the user must complete an age verification using a credit card. These settings can be adjusted in the plan and subscription settings.

More information: https://ee.co.uk/help/cyber-security/getting-started/switching-content-lock-on-or-off#article-heading-2

iD Mobile

iD Mobile have a way to activate content restrictions on devices. Accessing an age restricted website such as gambling will redirect to the iD Mobile content control webpage. It is possible to add and remove these restrictions in the iD app or in the 'my account' area. Then select 'services' and then toggle adult content filtering 'on' or 'off'.

More information: https://www.idmobile.co.uk/help-and-advice/content-control-information

O2

The age restrictions are set by default, blocking 18+ websites. They are usually blocked by a 'Timed out' or 'No Response' message. Much like the other mobile network providers they have a ranking of how much they filter.

More information: https://www.o2.co.uk/help/safety-and-security/age-restricted-content-and-age-verification

Other Mobile Network Providers

Most mobile network providers offer the same type of filtering for their own SIM cards. Here are the guides for more mobile network providers:

Sky Mobile: https://www.sky.com/help/articles/parental-controls-sky-mobile

Tesco Mobile: https://www.tescomobile.com/help/safety-and-security/parental-controls-and-content-settings

Virgin Media: https://www.virginmedia.com/broadband/parental-control

Vodafone: https://www.vodafone.co.uk/support/articles/how-do-i-change-my-age-restricted-content-settings----83107c7f-350a-4279-aab8-34a0709a5d8e

Teams/School Accounts

With some school lessons based online, the security of a work or school account has become even more important. Security can be improved by having a secure password and enabling multi-factor authentication. The National Cyber Security Centre's (NCSC) advice is to use a password made up of three random words. This is because longer passwords are harder to crack than shorter, more complex passwords.

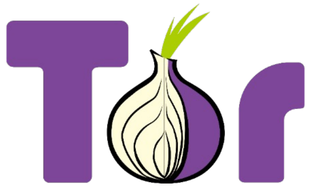
https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

In addition to using a strong password, multi-factor authentication (MFA) should be enabled on your accounts. For Microsoft Teams accounts, this can be done through the Microsoft Authenticator App. After inputting your password to your Microsoft account, the app will prompt you to confirm your login before allowing access to your Microsoft account.

Password Managers

Password managers are a tool that stores all of your passwords in a vault. Accessing this vault requires a master password. This can be a valuable resource, as remembering numerous complex passwords is difficult. With a password manager, you only need to remember one password. Password managers have a variety of features, such as password generator, automatic insertion of username and password, and warnings of reused passwords. Alongside this, most password managers can be used across multiple devices.

There are many password managers available, including LastPass, DashLane, Keypass, Google Password Manager, SamsungPass and Apple Password Manager.

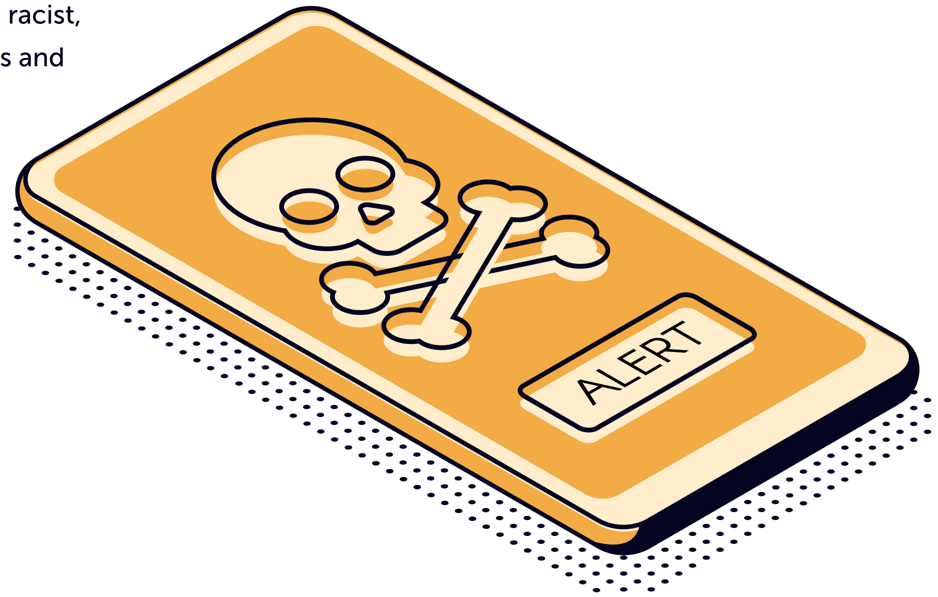


Tor Web Browser

The Tor Browser, developed by the Tor Project, promotes anonymity while users navigate the internet. However, it can also be used to access the 'Dark Web' or 'Darknet'. This is a 'hidden' part of the internet that is not accessible through regular browsers but can be reached via Tor. Pages on the Dark Web may contain illicit or dangerous information, and content that is not appropriate for children. There is no legitimate reason for a child to have the Tor Browser on their device, so if you notice an icon like the one above or the software itself present on their device, it is worthwhile discussing this.

Unsafe Online Forums

Online forums allow users to discuss topics of interest, such as games, movies, or other legitimate subjects. However, some forums can be potentially dangerous and contain explicit content inappropriate for children. One example is 4chan, a forum which has been linked to racist, homophobic, and sexist messages and groups.



CYBER
AND FRAUD
HUB

☎ 0808 281 3580
✉ info@cyberfraudhub.org
⌂ cyberfraudhub.org
@cyberfraudhub
in cyber-and-fraud-hub

Registered in Scotland. Registered Charity No.SC053371