Staying safe online

Advice for Parents and Carers

Scottish Business Resilience Centre

Safety Guide.

Nowadays, children are just as adept at using the internet as adults, and in some cases, even more so.

With all the amazing learning opportunities and collaboration that the online world brings, sadly, there's also a much darker side to the internet and it's important we teach our children about measures they can put in place to ensure their safety.

SBRC's ethical hacking team have put together this guidance document aimed at parents and carers to help them better understand the potential risks and controls around popular online sites and platforms.

This guide is intended as advice only, more information can be found on the respective websites of the platforms mentioned later in this guide.

If you have any questions, please email:
enquiries@sbrcentre.co.uk

Contents:

Online Safety and Gaming

Internet Trends

An internet trend is something which is popular online, like the ALS ice bucket challenge in 2014. Trends can be simple and positive, the ice bucket challenge raised a lot of money for ALS, however trends can also be destructive. One such trend was the salt and ice challenge whereby people held ice and salt to their skin. This causes a burn and could leave permanent damage.

It is important to talk to children about how not everything they see online is a good idea/true/real.

Oversharing

Video games that have online capability often have text chat or voice chat. It is important that if your kids play online games, that they know the difference between what they can talk about with strangers and what they can talk about with friends they REALLY know.

Do not give out:

- **Home address**
- **Phone number**
- **Full name**
- **Age**
- **Which school you attend**
- **Anything unique to where you live**

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

Grooming

A groomer is an extremely dangerous individual who tries to become close to someone to get something out of it.

For example:

- **Sexual conversations**
- **Sexual images/videos**
- **Sexual video calls**
- **Meeting up in real life**

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

The signs to look 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 physical appearance**
- **They give compliments about how mature the person they are chatting to is**

It is important to know who your children are talking to online, but you can only keep an eye on them so much.

It is much more important that they know and understand the dangers themselves.

Age Ratings

Video games age ratings

86% of parents claim they do not really follow the age restriction on video games.

The obvious problem is that some games contain inappropriate content for children. This can include not only graphic violence, but also profanity, drugs, and sexual content.

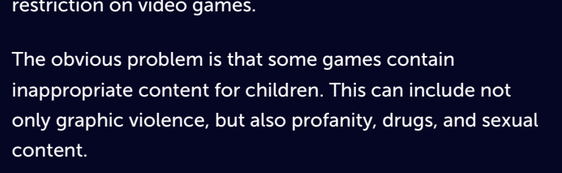
However, in the online age there is a darker side. If you buy an 18 rated online game, your child is going to be playing with people who are (mostly) 18 or older. This means adults will talk like they are with adults. Your child may hear profanities or pick-up language or sayings which may not be appropriate.

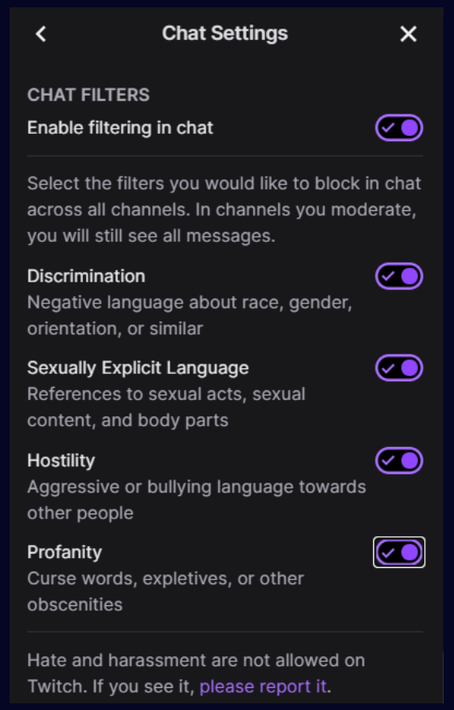
Twitch

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 watcher, 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 which watch out for anything that goes against the stream's rules.

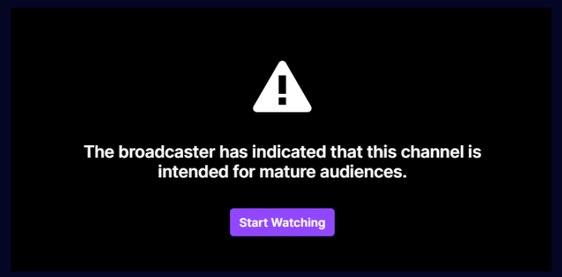
There is an option to enable chat filtering for profanity and other topics. Enabling this could be a good idea for younger viewers.



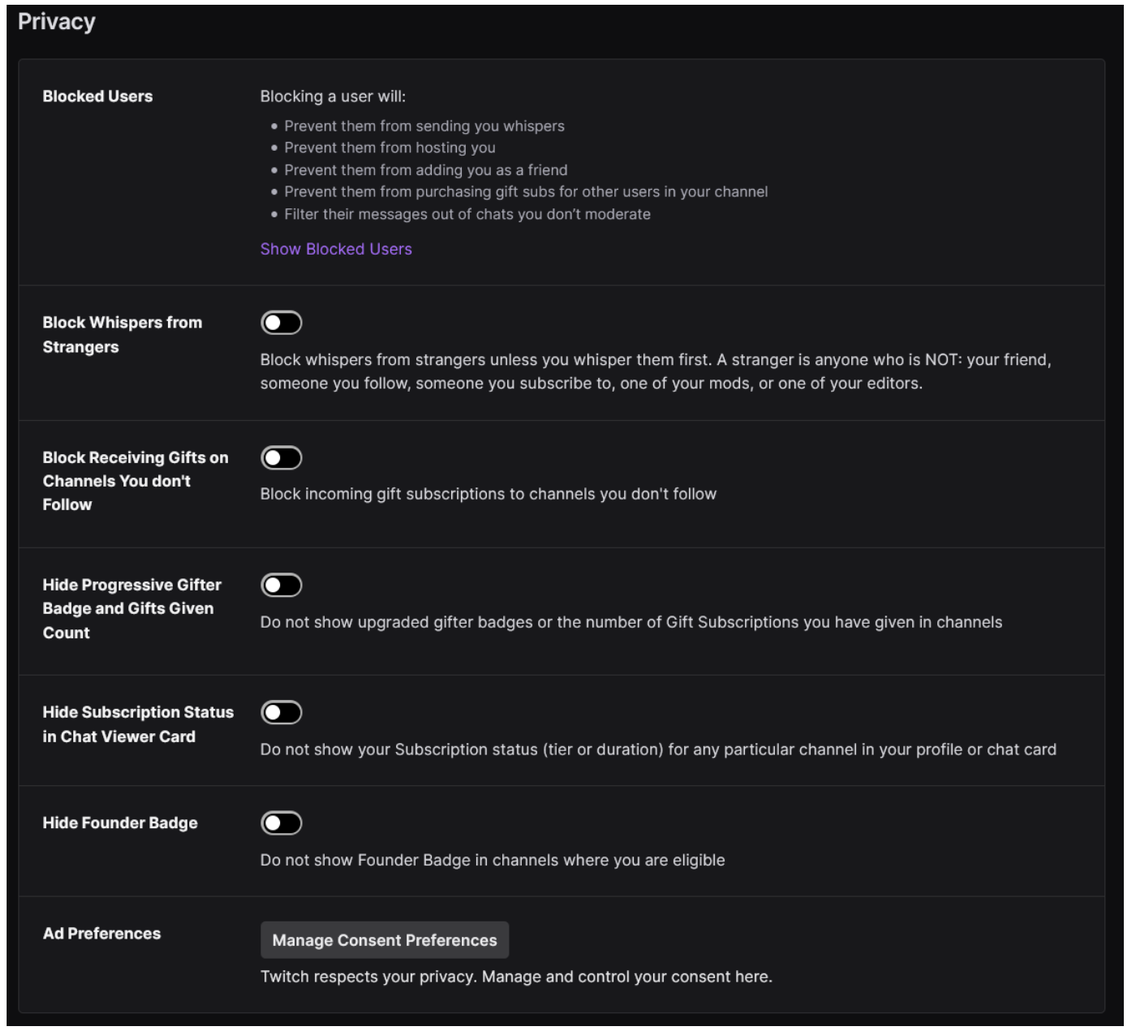


Twitch has a large variety of streamers aimed at a range of different audiences. If the game they are watching has an age rating of 16-18 it is likely the stream is aimed at an older audience.

Twitch streamers sometimes include a warning about how the stream is intended for "mature audiences". This warning is easy to bypass. This is why it is important to check if the streamer is appropriate for your child.



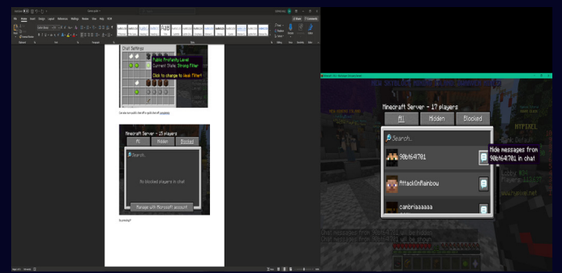
There are several options for privacy. Users can block other users; they can also block private messages (called "whispers" on Twitch) from strangers.



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

Minecraft

On Minecraft (Java edition), there is a multiplayer option. By joining a server, they 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.



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

Users talk to each other in the chat. Some servers have completely unmoderated chat. The chat can be completely 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 online from working.

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 hot bar. By right clicking while holding it, a menu is opened.

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 different profanity levels are available for different groups of players.

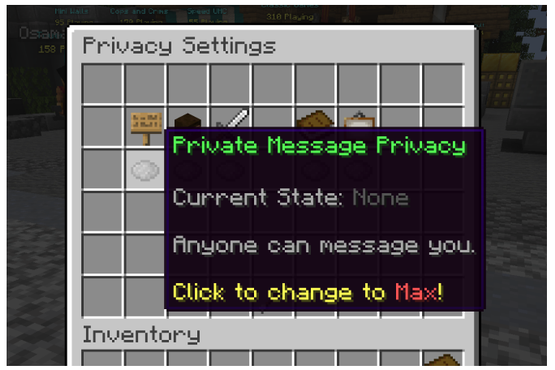
By clicking on “Privacy Settings” Users can change their privacy settings.

There are privacy settings for:

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

For example, private message settings can be set to:

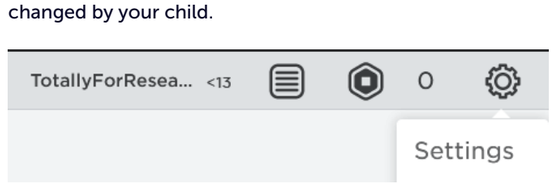
- **Anyone can message you**
- **Staff, friends and guild members and party members can message you**
- **Staff, friends and guild members can message you**
- **Staff and friends can message you**
- **Only staff can message you**



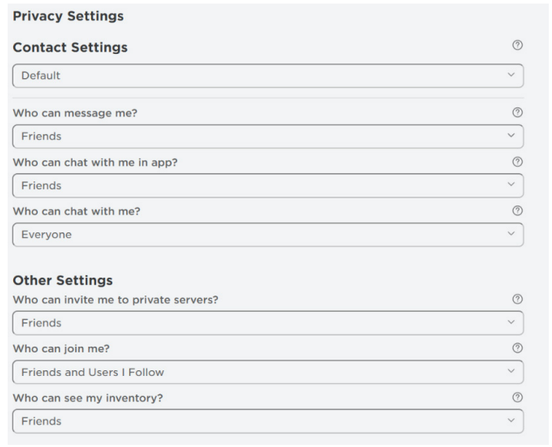
It is also possible to link social media accounts. This includes Twitter, Discord, YouTube, Instagram, etc. Once added anyone can see this information, so it’s important to not allow this.

Roblox

Roblox allows for users to join servers to play with others. It is popular on mobile devices, PC and Xbox. Roblox allows for parental controls where they have plenty of control. These options can be put behind a pin so they cannot be changed by your child.

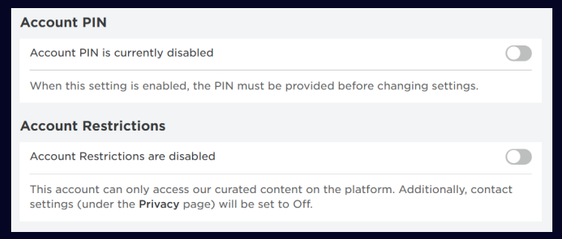


Privacy settings can be changed so only certain users can message your child and that only certain users can invite your child to play with them.



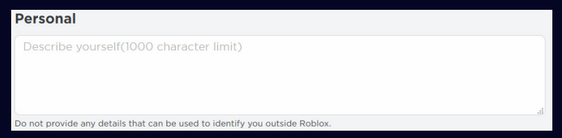
An account PIN can be added to stop your child changing the settings you have set.

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



Users can be blocked by going to their page.

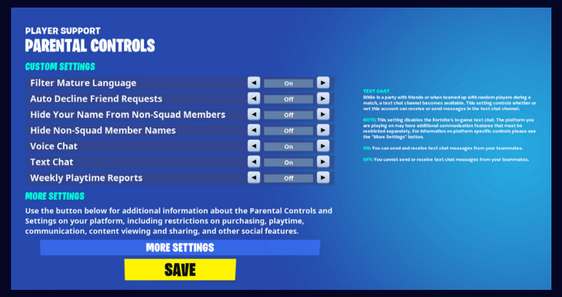
Parents should keep an eye on what is put in the personal bio section. It is never a good idea to include anything identifiable.



Fortnite: Battle Royale

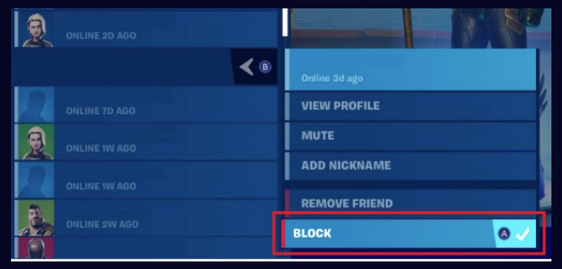
Fortnite is an online game where the aim is to stay alive while eradicating the other players/teams/monsters. The game is violent, but it is not gory.

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



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.

Players can also be blocked in the social tab.



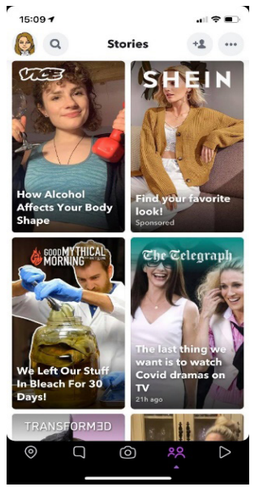
Social Media Guidance for Parents

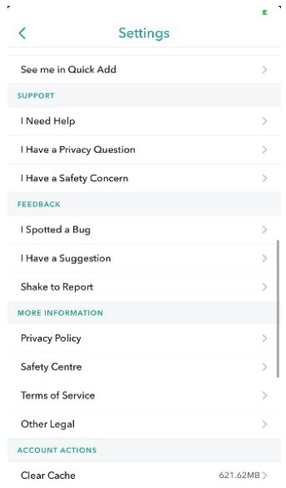
Snapchat

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

Features include:

- **"SnapMaps" – a feature where users can share their location in real-time with their friends and see other users who have the same feature enabled. This feature can be dangerous as 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 - a section of Snapchat that displays popular articles from various medias. These can sometimes contain explicit content that is not appropriate for children.**





- **Stories - a space where multiple Snapchats can be added that can be viewed for 24 hours. Users can also create private stories where they can select what friends can view this story. It is possible for users to block other users from viewing their story by going to Settings > View My Story > Custom.**
- **Quick add - this shows friends of friends that users may know and may be interested in adding. This allows users to see your username and attempt to add you. This can be turned off in Settings > See Me in Quick Add.**

Age Restrictions and Prevention

Due to the nature of messages, pictures and videos deleting, Snapchat can be hard to monitor to protect your child. Bullying can be difficult to detect also.

Make sure to have a conversation with your child to let them know of the risks and let them know they should save any harmful messages on the chat or screenshot any hurtful pictures.

The age restriction on snapchat is 13, and during sign-up, users are asked for a birth date to ensure this. Children may, however, go around this by entering in 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.

Top tips for staying safe:

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 Snapchat, story or account.

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 three seconds to one minute. The platform was originally aimed at children, however, the app has recently grown in popularity and tailors to users of all ages.

Features

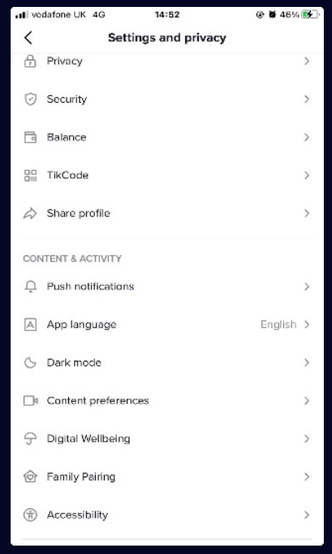
- The 'For You Page' is randomly generated by an algorithm that displays content that suits the user. Videos that are shown are picked based upon what the users viewing is generally like, and picks videos that are popular and similar to already viewed and liked content.
- The 'Following' Page will display videos belonging to an account that the user follows.
- Users can 'Duet' videos created and respond to them, sing along etc in a side-by-side comparison. There is also an option for users to "Stitch" videos. This is where others can take a video, edit the start of it and add on their own content in reply to it.
- Users can also direct message on TikTok and share videos with one another.
- Live streaming allows for users to video themselves live, and have people watch real-time and comment/ interact with the user.

Age Restrictions and Prevention

The age restriction on TikTok is 13, however there are ways around this for younger children to create accounts. TikTok also bans accounts where owners are considered/reported to be under 13. If the user of the account is between 13-15 years old, their accounts are automatically set to private, only friends can comment and other users cannot duet, stitch or download videos by these underage users.

Top tips for staying safe:

- A strong password is always important and TikTok now has Two-Factor Authentication, security alerts for suspicious activity and users can check what devices they are logged into.
- The privacy section in settings has many options to private a user's account, block direct messages, comment filters and determine 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 sees, track their watch time and change their child's account to private. This can be found in Settings > Family Pairing. It easily set-up by linking the accounts together with a QR code.



- There is an age limit on live streaming, which is 16, however, teens should ensure that if they are going live on a public profile, that they're not revealing too much information such as where they live, where they go to school and any other private information

Instagram

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

Features

- Stories are images/videos that a user can upload which will disappear after 24 hours. There is no 'like' feature on these, and other users can only comment/react through direct message. Stories can be viewed by anyone if a user's profile is public.
- Reels are like TikTok. Users can record themselves, add music/effects to a 15 second clips.
- 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), this is where longer videos can be posted on Instagram. They can be viewed in more of a 'explore' feed form, so users will see posts not necessarily by their friends/followers.
- Users can also live stream themselves in real time and have their followers watch them and interact through commenting or going live with them, like a public Facetime.

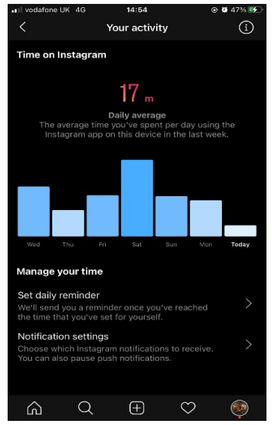
Age Restrictions and Prevention

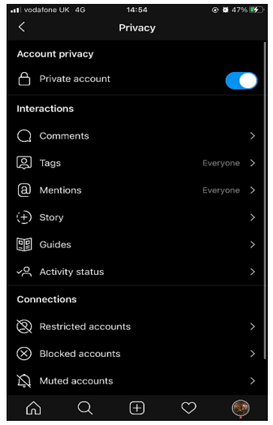
In the Instagram terms of service, the age restriction is 13 years old, however there's no process to verify this. Therefore, many children easily create an Instagram account.

The content 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 other posts about concerning topics. Adverts are also displayed which cannot be controlled and tailor to the user's online activity, so it is possible for inappropriate adverts to be displayed.

Top tips for staying safe:

- Set up Two-Factor Authentication on Instagram by going to Settings > Security > Two-Factor Authentication.
- Children/teens may want to consider setting their accounts to private for their own personal safety, especially if they post pictures with revealing information such as where they live, go to school and their daily routine.
- Comment controls can be added to restrict comments from followers only, as well as blocking comments with specific words.
- Users can stop 'resharing', this is where other users can share someone's story onto their own story.
- Users can set a time limit on how long they are spending on the app by going to Setting s > Your Activity > Set Daily Reminder. This will only alert the user when they have reached the time, however, not actually restrict them from staying on any longer.





Facebook

Facebook is a social media platform where users can share photos, videos, and status updates with their friends.

Features

- **Users all have profiles that can show their names, place of study and where they're from. However, the privacy settings are completely customable to each individual user.**
- **Messenger is connected to Facebook as its messaging app; although it can be used on its own and a Facebook profile is not required to have Messenger.**

Age Restrictions and Prevention

Facebook requires everyone to be at least 13 years old before they can create an account. Facebook state they will promptly delete the account of any child under the age of 13 that's reported to them.

Top tips for staying safe:

- **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 children/teens only add people they know and trust. A lot of explicit and unsafe content can be shared around Facebook, but this will depend on what a user's friends share and the pages they follow.**
- **A lot of revealing information can show on a user's Facebook profile, including family members, place of birth, where they currently live, jobs and education history. It is advised to have this information, if it is on your profile, to not be public for anyone to see. This can be modified by going to Settings > Privacy > Manage your Profile / Your activity / How people can find and contact you.**

Twitter

Twitter is a social media site and app that lets you post messages called "tweets". These can be up to 280 characters long. As well as tweets, you can send private messages and post pictures and videos. You can also livestream on Twitter.

Age Restrictions and Prevention

Twitter requires people using the service to be 13 years of age or older. Content that appears on Twitter is very much dependent on who a user follows. However, many child-friendly content creators do not have child friendly Twitter pages.

Top tips for staying safe:

- **Set up Two-Factor Authentication by going to Settings and Privacy > Account > Security > Two Factor Authentication**
- **Set the profile to private, this is especially important if any tweets made reveal any personal information that not just anyone can see. This can be done by going to Settings and Privacy > Privacy and Safety > Protect your Tweets.**
- **Twitter has a feature where users can tag their location in their tweets. Children/teenagers should steer away from using this feature for their safety, especially if their profile is public.**

YouTube

YouTube is an online video sharing platform. It has hugely diverse content from vloggers, gamers and educational videos.

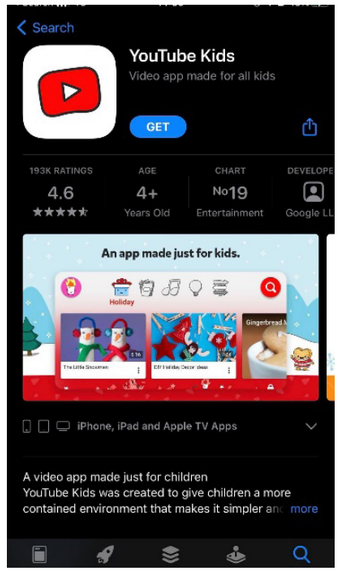
Anyone can upload videos and similarly anyone can watch public videos. There can be lots of inappropriate content on YouTube for children, however there are many ways to control this.

Age Restrictions and Prevention

YouTube isn't meant for anyone under the age of 13, however, that doesn't always stop young children from using the app at home or elsewhere.

YouTube's trust and safety team applies restrictions to videos when they come across them during reviews. If it's deemed inappropriate for people under 18, it gets an age gate.

There is a separate version of YouTube called YouTubeKids that has pre-filtered content that is only suitable for children. There are lots of controls so parents can cap screen time, volume and the search function.



Top tips for staying safe:

- **Check who your children and subscribed to and encourage them to stick to these creators. This would prevent children from searching through YouTube for content and potentially coming across inappropriate videos. They can get notifications for new videos from their subscriptions.**
- **If your child is uploading videos to YouTube, ensure that they are not revealing too much information. Such as where they live, what school they attend and their phone numbers. Give their videos a watch first before they upload or make their videos private/unlisted (only people with a link/are whitelisted can watch).**

Discord

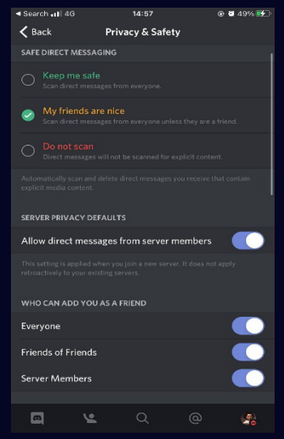
Discord is a platform for voice chat and instant messaging. Servers can be created to host multiple people. Sometimes discord servers are public for certain game servers and anyone can join. These are sometimes heavily moderated to ensure safety however users should be vigilante of who they are speaking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

Age Restrictions and 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 joining.

Top tips for staying safe:

- **To prevent children getting inappropriate direct messages, there is a feature that can be turned on that will scan direct messages for inappropriate content. This can be changed by going to Your Profile > Privacy and Safety > Selecting either Keep me safe, or My friends are Nice.**
- **It is also possible to restrict on who can direct message you in the first place 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 if they already know their friends who they talk with online.

General warnings

- Parents and children should be vigilant of who they speak with online, sometimes people disguise their profiles pretending to be other children, so caution is advised on what information users give out to each other.
- Children should be advised not to give out information such as full names, pictures of themselves, where they are from and what school they attend.
- When filming videos/taking pictures of themselves, children should be cautious of any revealing information in the background when sharing them with strangers online, such as TikTok videos showing addresses, wearing school uniform and sharing pictures of houses that may be identifiable.
- A common trend online (especially on TikTok) is lifehacks. These can be relatively harmless most of the time. However, there is an influx online of lifehacks without sufficient warnings attached to them. Watch for things like dangerous mixing of chemicals or test dropping mobile phones.

Cyber Bullying

- Cyber Bullying can be common online and severely detrimental to mental health. Parents should check up on their children regularly if they experience any relentless and serious abuse online. If it does occur, users should block the offending user/private their account if it is not already. Everything that is said should be documented, then reported to the platform it is taking place on. If a child also knows the person in real life who is bullying them, it can be reported to the school and in serious cases, the police.
- Cyber Bullying can present itself as direct messages and posts towards the victim but can also be indirect taunting online, such as the spreading of images, abuse and mean messages.

WhatsApp

WhatsApp is a messaging application used to send text messages, voice notes, and video/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.

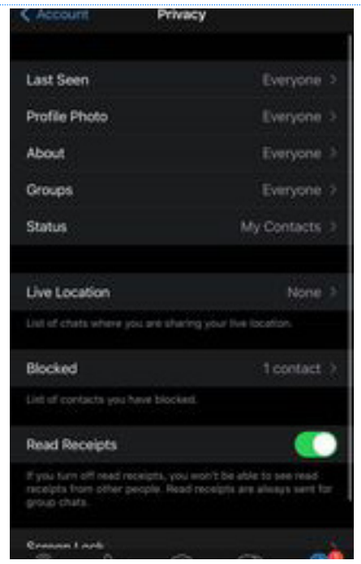
Age Restrictions and Prevention

The minimum age of use on WhatsApp is 16 years old, however many people of a younger age have profiles.

Top tips for staying safe:

- Due to WhatsApp using phone numbers in order for users to contact each other, it is a relatively friendly way for people to contact one another as long as the number is not public anywhere. However, ensure that your child adjusts their settings so only contacts can add them to prevent them from receiving messages from strangers. This can be done by going to Settings > Account > Groups.

- WhatsApp also has a default setting that will automatically download media that is sent and interacted with. In order to prevent your child from downloading an inappropriate photo, turn off this setting go to Settings > Chats > Save To Camera Roll.
- Live Location is a feature where users can turn on sharing their current location. Make sure this is only on with absolute trust and if completely necessary.



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.

The Admin Panel

Once you've accessed the admin panel for your ISP, 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.

Adding Parental Controls to the Router

BT

To gain parental controls, within the BT hub system, an addon 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, they will begin working within two hours. The management of these can be done within your MyBT account.

Sky

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 onto the device. These controls can be implemented to prevent app store purchases, restrict the game centre, as well as restricting the web content that can be viewed.

To access these settings, 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 – this restricts Siri from searching the web and displaying explicit language.

Restrict Game Center – 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, unlike Apple, has no parental control settings built into the system. However, there are parental controls for the Google Play Store, and Google has an application to enforce parental controls.

The Google Play parental controls can be set up by going into the settings of Google Play and navigating to parental controls. Once there, you set up a pin and the restriction level that 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 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.

Most modern browsers include the ability to add extensions. These extensions can range from a tab manager to study aids. These extensions can also upgrade the privacy and security of the browser. For example, they can delete malicious/tracking cookies and block ads. The use of these extensions allows for greater privacy while browsing the internet.

Some of the top-rated privacy extensions are:

- **uBlock Origin – this extension blocks adverts within the browser, some of which contain trackers. These can track your browsing across web pages. As well as this uBlock Origin blocks known malicious adverting (the use of online advertising to spread malware) 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 addon blocks Facebook from tracking you around the internet, even when not on the site.**

Another privacy focused change would be to use DuckDuckGo for a search engine. DuckDuckGo is a privacy focused search engine and doesn't use your data to display targeted ads to its users.

Chrome

Chrome has some great extensions for both privacy and productivity. To access the Chrome Store where you can add these extensions, along with many other tools to Chrome, go to the 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

Teams and School Accounts

With schooling being online, the security of a work or school account becomes even more important. This can be done by having a secure password and enabling multi-factor authentication. The National Cyber Security Centre (NCSC) advice is to use a passphrase, instead of a password, consisting of three random words. This is due to a longer password being harder to crack than a shorter more complex password.

For more information, visit:

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

As well as having a strong password multi-factor authentication should be used 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 require you to confirm your login before allowing access to the Microsoft account.

Password Managers

Password managers are tools that stores all your passwords in a vault. To access, there is a master password, which unlocks said vault. This is a useful tool to use, as remembering tons of complex passwords is difficult. With the use of a password manager, only one password is required to be remembered.

Password managers have a variety of features, such as password generator, automatic insertion of username and password, and warnings of reused passwords. Along with this, most password managers have the ability to be used across multiple devices.

A whole range of password managers exist, some examples are, LastPass, DashLane, Keypass, Google Password Manager, SamsungPass, and Apple's Keychain.

Scottish Business Resilience Centre

Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

01786 447 441
enquiries@sbrcentre.co.uk
www.sbrcentre.co.uk
@SBRC_Scotland

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27