A PARENTS GUIDE TO DEVICE SAFETY 2.0

2nd Edition

Donegal Youth Service
Youth Work Ireland

Eolas Don Óga
YOUTH INFORMATION

Information you can trust

Donegal Youth Service
Youth Work Ireland

The following information is brought to you by Donegal Youth Service. This booklet is a fully researched and updated range of information on how to keep children safe online and how to protect their personal information from predators and hackers. Donegal Youth Service also provide a range of information workshops to different age groups including:

-Primary School Workshops

-Secondary School Presentations

-Parents Evening Information Sessions

For further information or to book contact:

Gareth.gibson@donegalyouthservice.ie
www.donegalyouthservice.ie

(074) 912 9630

Youth Information Centre
16-18 Port Road, Letterkenny

Contents

Mobile Phones and Tablets	Page 4
Securing your device	Page 5 - 8
Parental Controls	Page 9 - 11
Emails & Scams	Page 12 - 13
Dangerous Apps	Page 14 - 17
Social Media	Page 18
Facebook	Page 19 - 22
Instagram	Page 23 - 26
TikTok	Page 27 - 30
Twitter/X	Page 31 - 33
Snapchat	Page34 - 37
Discord	Page 38 - 40
Consoles	Page 41
PlayStation 4	Page 42 - 45
PlayStation 5	Page 46 - 49
Xbox One S/X	Page 50 - 53
Xbox Series S/X	Page 54 - 56
Nintendo Switch	Page 57 - 61

Donegal Youth Service
Youth Work Ireland

Mobile Phones and Tablets

Securing your devices

The rapid development of portable devices over the last few decades has led to a world where we have become reliant on them for a multitude of day-to-day activities such as surfing the web, setting up reminders, sharing files, social media, video calling, and even mobile banking.

Unfortunately, this increase in functionality has made our devices more appealing to criminals and vulnerable to online and physical threats. Some of these threats include malicious software, unauthorised access and even theft.

But it's not all doom and gloom. Here is a list of things you can do to minimise the dangers and keep your families devices and information safe.

1. Use a strong password or biometrics

Using strong passwords or biometrics like a finger print authenticator will drastically reduce the chances of unauthorised access. A strong password should be 12 characters or more and include capitals and lower case letters, numbers and symbols. Try not to make the password easy to guess, the more complicated the better.

Time it takes to crack a password

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

If you have difficulty remembering passwords, consider using a password management tool like bitwarden or lastpass which can store your passwords in a safe and secure manner. It is also a good idea to use 2 factor authentication (2FA). This adds a second method of authentication to the log in process which increases the difficulty when trying to gain unauthorised access.

2. Make sure public or free wifi is protected

Everyone loves free wifi especially when they have a limited data plan but these wifi points don't tend to be very secure and cybercriminals know this all too well.

To protect against wifi hacking, use

applications that secure your connection or tell you the status of the wifi to which you are connected. WPA (Wifi Protected Access) is more secure than WEP (Wired Equivalent Privacy).

It is also a good idea to turn off your wifi and Bluetooth when not in use. This will not only prevent automatic connection to unsecure devices but has the added benefit of reducing the strain on your battery .

3. Use a VPN

Using a VPN (Virtual Private Network) should be mandatory when you are using a network that you are not sure of the security in place. A VPN will scramble your data so no one can spy on your internet activity and will protect you on unsecure sites. VPN services are not overly expensive these days and some companies offer family plans to protect multiple devices.

4. Encrypt your device

It may seem a little excessive but if you are worried about you data being leaked if your device is stolen, encryption will negate this risk entirely.Most mobile devices come with encryption features which will scramble your data and decrypt or unscramble it when the correct password is entered.

It is important to know that encryption and decryption may slow down your device slightly but that is a small price to pay for piece of mind and you should also do regular backups of your data because if someone tries to guess your password too many times some applications will delete all the data to protect it.

5. Install an antivirus

Although Virus' for mobile devices aren't as common as those for Pcs they do exist so it's a good idea to protect against them by installing a reputable antivirus application. It is also good to know that some antivirus software offers additional features like tracking your device or wiping it's data if it is stolen or cleaning up uneccessary files from taking up memory on your device.

6. Update your devices software

No piece of software is perfect and loopholes that can be exploited are being discovered all the time so it is important to run updates as soon as possible because they often contain patches to these exploits which will help keep your device safe.

7. Use the internet wisely

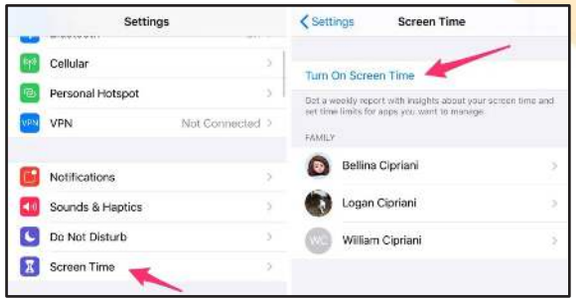
One of the best ways to stay safe online is to be discerning about what you do. Don't click on links from unknown senders, don't download software from unknown sources, and don't provide personal information to unconfirmed sites or people.

8. Keep backups

Unfortunately, no matter how careful we are, things can go wrong. One mistake can lead to your device becoming

compromised which may not just cost you money but could result in losing important contacts or cherished photo memories. A backup will allow you to restore this important data and a regular automatic backup can be scheduled for times you aren't using your phone lilke when you are asleep. Save your backup to an online service like Google Drive or iCloud so that it is accessible wherever and whenever you need it.

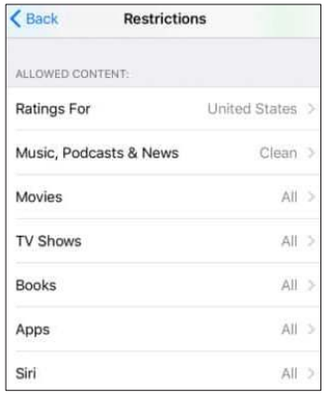
Parental Controls

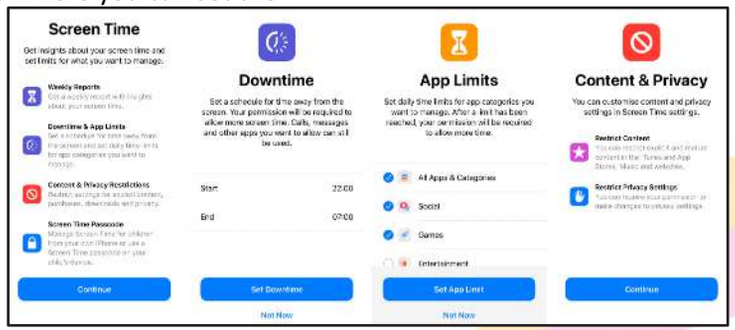


How to set up parental controls on an iPhone

Setting up parental controls on an iPhone is an important step to protect your child from accessing inappropriate content or using apps that are not age-appropriate. Here's how to set up parental controls on an iPhone.

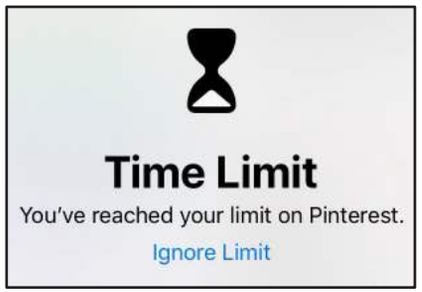
1. Go to Settings on your iPhone and select Screen Time.
2. Tap on "Turn On Screen Time"
3. Choose "This is My Child's iPhone"
4. From here you can set the restrictions of the iPhone including, age of user, hours on apps and ratings of TV Shows and Movies watched on the iPhone.





5. Scroll to the bottom and tap to turn restrictions on.
6. Choose the Downtime you want to use. This will prevent the iPhone from accessing certain entertainment apps. The default time should be between 10pm and 7am.
7. You can also set up individual time restrictions for specific apps and websites.
8. The last step is to create a passcode then you must input your Apple ID.

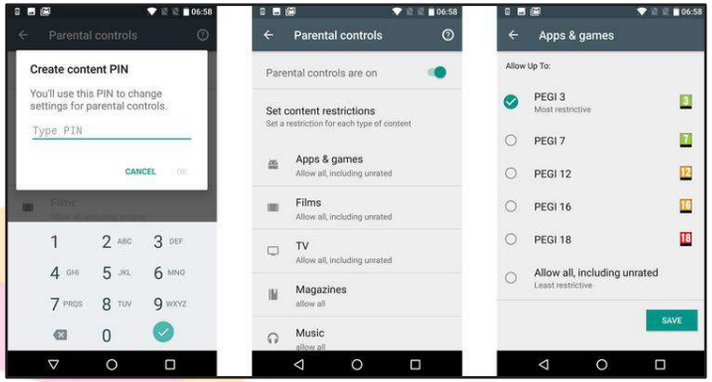
Once you've set up parental controls, you can manage them by going to Screen Time in your iPhone's settings. From there, you can see your child's activity report and make changes to the



restrictions if necessary. It's important to have open communication with your child about why you're setting up these controls and to monitor their activity regularly.

How to set up parental controls on an Android phone

Adding Parental Controls to your child's Android phone is an excellent way to ensure that your children are safe while they browse the internet or use any other apps on their device. Here are the steps to set up the parental controls on an Android phone:



1. Open the Google Play Store app on your child's device and tap on the avatar icon for the child's Email on the top right.
2. Scroll down and select 'Settings'.
3. Tap on the 'Family' menu then tap "Parental Controls" and then tap to 'Turn on Parental Controls'.
4. Create a PIN code that only you know.
5. You can set age restrictions for the type of Apps and Games as well as Films viewed and downloaded on the Android.
6. Once you have chosen the restrictions, tap on "Save" to enable the parental controls.

That's it! With these simple steps, you can easily set up parental controls on an Android phone to protect your children from accessing inappropriate content. It is important to note that parental controls are not foolproof and it is still important to monitor your child's phone usage and have open communication about internet safety. It should also be noted that your child can request to stop supervision but it will result in their phone being locked for 24 hours and the parent being notified.

Emails & Scams

How to set up an Email account

Setting up an email account is straightforward. Here are the general steps to follow:

1. Choose an email provider: There are several email providers out there, such as Gmail and Microsoft. Choose the one that suits your needs and preferences.
2. Go to the provider's website
3. Click on the sign-up button: Look for the sign-up or create an account button on the website's homepage. Click on it.
4. Fill in your details: You will be asked to provide some personal information, such as your name, date of birth, and gender. You will also need to choose a username and password. Make sure to choose a strong password that is not easy to guess.
5. Verify your account: After filling in your details, your email provider

will send you a verification link to an existing email or phone number. Click on the link to verify your account.

6. Set up your profile: Once your account is verified, you can log in and set up your profile. You can add a profile picture, create a signature, and customize your email settings etc.

7. Start sending and receiving emails: Congratulations! You have successfully set up your email account. You can now start sending and receiving emails from this account.

Remember to keep your password safe and secure. Also, be mindful of phishing emails and scams, and never share your personal information with anyone.

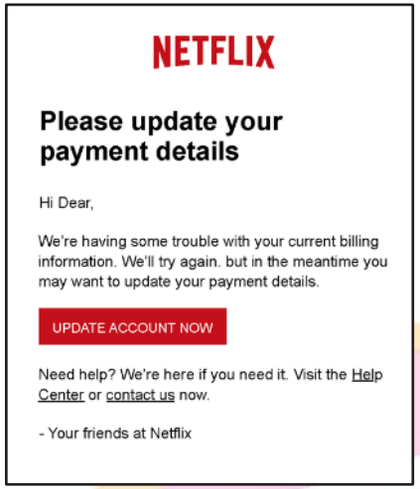
What are scam emails?

Scam emails, also known as phishing emails, are fraudulent emails that are sent to unsuspecting individuals with the intent of stealing their personal and/or financial information. These emails often appear to be from legitimate sources, such as banks, social media platforms, or other organisations, and may request that the recipient provide sensitive information, such as passwords, social security numbers, or credit card numbers.

Scammers use a variety of tactics to make these emails appear legitimate, such as using official logos and branding, and creating urgency by claiming

that the recipient's account has been compromised or that they are at risk of losing access to important services.

It's important to be cautious when receiving emails from unknown senders or emails that seem suspicious. Always double-check the sender's email address and be wary of any requests for sensitive information. If you're unsure about the legitimacy of an email, it's best to contact the organisation directly through their official website or customer service channels.



Dangerous Apps

It's fair to say that any app that allows communication with others has inherent risks and dangers when it comes to young people but the following is a list of some apps that have functionality that can be abused and parent should at least be aware of these risks so they can discuss them with their children.

Snapchat

This app has become incredibly popular these days with millions of users but It has the risk of young people becoming complacent with what they post because of their messages disappearing after a set amount of time.

Omegle

This is a video chatting app that lets you have video chats with strangers online. The app has become popular with curious kids and has lead to some being subjected to people exposing themselves and sexual predators.

TikTok

This app is by far one of the most popular apps at the moment with over 500 million users worldwide. Although the app is intended for people over 13 years of age there is no age verification and there is nothing to stop someone under that age setting up an account. A lot of the videos include innappropriate language and some dangerous challenges which have led to a number of deaths. It should also be stated that all accounts are made public as default so potentially a young person aged under 13 could be contacted by a predatory adult.

Whisper

This is a "confession" app that allows users to confess to things anonymously online. Users can communicate with other users nearby and uses GPS to track who is nearby. The app does keep users identity anonymous but it does show the location that a message was sent from and has been used to track and assault an underage girl by a sexual predator.

Kik Messenger

Kik messenger was initially designed to make chat messenging more fun and engaging. The app can be used to send pictures and texts but has no age verification. As a result of this, the app has been used by stalkers and pedophiles to groom young people and convince them to share innappropriate images.

Tinder

Tinder is another popular app for finding and conversing with people and uses GPS to track nearby users. This app is especially popular with teens and tweens and a such has been used by pedophiles creating fake accounts to lure young people into dangerous situations.

Ask.fm

This app allows it's users to ask questions either anonymously or as themselves. The ability to ask and answer anonymously has given rise to users asking vulgar questions or providing grossly innappropriate and offensive answers. This app has also been associated with a number of cases of cyberbullying.

Instagram

Another popular photo sharing app with about 2.3 billion users, it has become the target of hackers. There is also a large amount of innappropriate content on the platform

Telegram

Telegrams main selling point is its self deleting messages. This functionality is giving rise to a lot of adult content being shared even amongst young users which can be difficult for adults to monitor. There is also the issue that usernames are public and can be searched which could lead to children communicating with strangers.

Tellonym

This app refers to itself as "the most honest place on the internet" and allows kids to reply to questions anonymously. As a result of this functionality it is not uncommon to witness cyberbullying, threats of violence and even sexually explicit content.

Blendr

Blendr is very similar to tinder in that it allows people to flirt and chat with others in a certain radius. And much like Tinder it is being exploited by pedophiles to track and communixcate with young people.

Houseparty

Houseparty is an app that allows users to communicate with one another via text and video chats. The videos can be streamed live so there is no way of telling what will be showed

Voxer

This is a “Push to talk” app that allows users to send and receive short voice messages very quickly. Voxer has a predominantly adult user base with people using it to communicate with colleagues at work but is becoming increasingly popular with teens. The user base is becoming more and more toxic with obscene or hateful messages becoming a common occurance.

Holla

Holla is a video chat app similar in nature to Omegle with all the associated dangers and pitfalls but Holla can use the devices location services to match you with someone nearby. This app has also become synonymous with violence, profanity and nudity.

Twitter/X

Often considered the most toxic of social media apps, it gives young people access to a lot of very innappropriate content and it doesn’t require a login to access anyof it.

Banuba

This app allows people to add face changers, filters and funny effects to pictures and videos. This app has a few concerns associated with it. It allows auto renewing of subscriptions for some of its services making it easy for a child that may not know what they are doing to run up some considerable bills, There are a large amount of adverts and pop ups used on the platform and it can be used to edit other peoples pictures and videos for the purposes of cyberbullying.

Bigo Live

Bigo Live is a live streaming app that allows people to showcase their talents and talk to people. More and more young people are streaming and creting blogs in the hopes of making money and a lot of the user generated content contains nudity profanity and violence.

WeChat

WeChat is a very popular Chinese multipurpose app that offers messaging, social media and payment services and has over a billion users. Former US president Donald Trump branded the app as a threat to national security and has made accusations of the app harvesting users data. How true this is we don’t really know.

VSCO

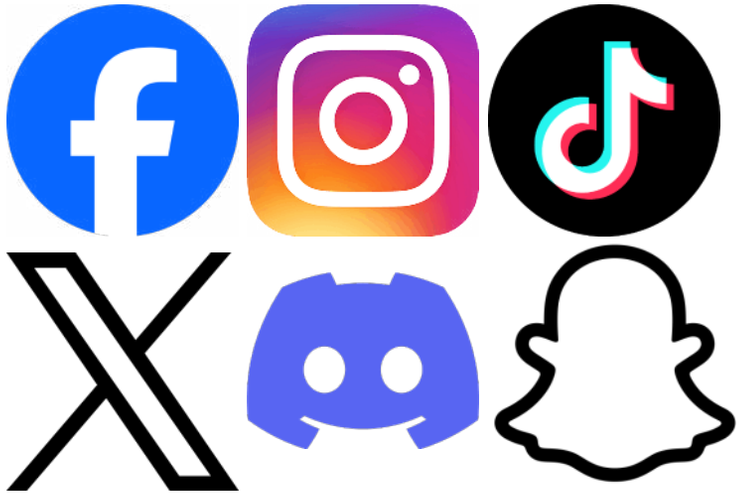
A photography app that offers users a variety of tools and filters to take, edit and upload your photos. The problems with this app are that the location and privacy settings are set to public as default and there are other tools available for sale that a young person could clock up a hefty bill if left unsupervised.

Tumblr

A part Blogging, part Social networking app it is often used by teens to share texts, images and videos but has been described as “too raunchy for tykes” by Common Sense Media. Innappropriate content such as violence and pornography are freely available through the platform. It should also be noted that accounts default as public and the process of setting up privacy is very complicated.

Vault apps

A set of apps rather than an individual app, they allow for a part of the phones memory to be partitioned off and hidden only allowing access when the right passcode is entered. These apps are often disguised as other programmes like calculators which makes it difficult to know they are even there and they can store messages, images and videos which can make it easy for kids to hide stuff from parents.



Social Media

Facebook

Easily one of the most popular media platforms in the world. However, with such a widespread appeal, there are dangers associated with the use of this platform especially by young people. One of the most obvious is the lack of Age Verification. Facebook trusts that its users give their real Date of Birth and as such it is easy to falsify this information. Meaning a child could make themselves appear older or an adult could make themselves appear younger.

The Addictive Nature of Facebook

One of the main reasons Facebook has become so popular is it's effective cycle of rewarding engagement. Likes and such feel good to get because it means your post is popular and reaching a lot of people but because they can happen at any time and be reached by almost anyone then it prompts users to check frequently by habit. The FOMO or Fear Of Missing Out is hardly a new phenomenon but it does drive up engagement by creating an environment where something is always happening and for a lot of young people it can be hard to ignore the pull of being in the know.

Cyberbullying on Facebook

While we'd all like to believe the best of others, the distant nature of Facebook as well as other social media platforms allows people to easily tease, antagonise and even torment a person with little to no recourse. While this activity can be reported, by that stage it could already be a case in which the damage has been done.

Future Impact

For better or worse everything that is put online stays there pretty much forever. Any embarrassing messages, pictures or public posts. It's all there and even private messages can be located and accessed. Some of which could really harm a person's reputation if it comes out and it is common for Employers and Universities to browse Facebook pages of potential employees or students.

Strangers

Easy access to Facebook means almost anyone can be contacted by almost anyone else and the reality is this means that those with malicious intent can try to contact potential victims. Friend

requests from people you do not know might be harmless, a misspelled name or a wrong click could be all it is but there is always the possibility that it is someone who means harm.

Sharing Too Much

Because Facebook survives on user content users are constantly encouraged to post and comment. This can lead young people to give away information that they do not intend such as their location, age or even home address if they are not careful.

Exposure to Inappropriate Content

While Facebook does monitor and remove certain inappropriate material, such as Hate Speech and extreme political opinions this information is not always taken down right away so there is a risk of a child running into it.

Fortunately advertisers are not permitted to use targeted ads on anyone under the age of 18 on the platform.

Livestreaming and Videos

Like many other platforms, Facebook allows the upload of videos and the live streaming of broadcasts on the platform as well as shorter "reels" which can be viewed on the site. A major factor of these is the difficulty in monitoring and regulating a live feed because anyone watching it can comment as well as possibly containing unsuitable content for young children or even content that encourages harmful behavior.

What can be done?

Use Private Accounts

Facebook allows any account to be set to private using the Settings Area. This is a safer way to for a child to use Facebook because it limits interaction to

between friends on the platform only. The settings can also be used to keep a child's personal information from being seen for example contact details and age.

Informed Sharing

Keeping a your child informed about the realities of sharing their posts can go a long way to keeping them safe. Letting them know the simple fact that what they post can be shared by others again and again that they might make safe choices in what they post. There is also an 'Audience Selector' option which allows users to restrict who can see their posts.

Being Safe with Friends

Be sure to let your child know about the possible risks of engaging with strangers on Facebook (and online in general) and before they accept a friend request to consider have they met this person in the flesh or do they trust them enough to allow them access. These might seem obvious but with the number of friends being seen as popularity by some it could be an easy thing to forget.

Establish Boundaries

It might be hard for some but trust is an important part of keeping your child safe. Once you have informed them of the dangers and what measures should be taken you will need to give them space to use these tools themselves. This serves the dual function of helping the child take charge of their own safety and allowing you to show trust in the child's judgement.

Don't just Tell, Show

Children often learn by example, long before they know the whys of many actions they learn the how. So by establishing a safe and comfortable presence on Facebook that your child can see you using they will be more accepting of limitations. Especially if they see you follow the same rules such as time limits or restricting access to your posts.

Use the Report and Block functions

Blocking certain users or groups can help keep the child from harmful influences and reporting inappropriate content can help keep the platform clear of such things. It is important that all users, young and old, know how to use these tools.

Instagram

As one of the most popular social media platforms Instagram allows users to send messages, stories and videos to each other from anywhere to anywhere on the platform. However there are risks involved.

Addiction

Instagram is designed to keep people engaged with the anticipation of what they might see next on their feed. This is good for the company as it keeps people logged in for longer but it can lead to losing track of time if one isn't careful.

Product Tagging

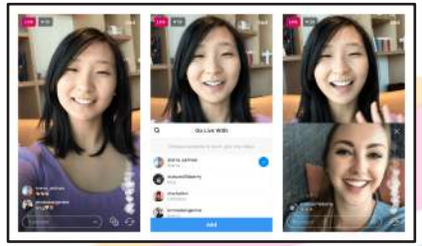
Product Tags allow a direct link to a products page and could encourage children to make unnecessary purchases or expose them to products that are inappropriate for their age group.

Exclusion/Ostracism

Exclusion is a powerful thing for children and it can affect them seriously if they are not being tagged or ignored in messages. This can be just as bad as offline exclusion in terms of children's wellbeing.

Public Accounts

Since Product Tagging only works on Public Accounts a child may be tempted to make their account visible to strangers in order to show off a product or style they are using. This can leave them vulnerable as their profile may include sensitive information or information used to discern their identity or home location.



Going Live

While going live allows children to instantly contact their friends in real time it can also open them up to offensive language, abuse or even people who might seek to harm them if their account is a public one.

Influencer Culture

Influencers are paid a lot of money to advertise products and often enter into temporary partnerships to encourage others to buy or use a product. This is an attractive idea to a lot of young people and it might lead to a young person acting inappropriately in order to gain the notoriety needed to get such a partnership.

Unrealistic Ideals

Many young people compare themselves to what they see and this can leave them with unhealthy expectations. This can lead to unhealthy actions that can seriously harm themselves.

What can be done?

Talk openly

Be candid about the potential risks involved in Going Live and other uses of Instagram. Educate the child on how they can be safer when using these tools and encourage them to come to you with any issues.

Take Away Payment Methods

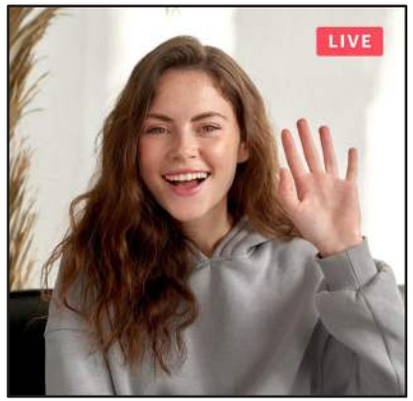
Keep card payment methods away from any Instagram account the child has. If you feel they are ready for that level of responsibility then it is strongly advised that a PIN code be implemented to add another level of security.

Use Moderators

“Live Moderators” are available from Instagram and are used to help give the user control to report commenters and even remove viewers from Live Events. Keeping a device in the open like the Kitchen or Living Room will help you stay aware of when it is being used to Go Live.

Get Familiar

On the Instagram website there is a Safety Features document specifically or Parents/Guardians benefit. If you familiarize yourself with this then you will be better equipped to know how to help keep your child safe when using Instagram.



Get to Know Influencers

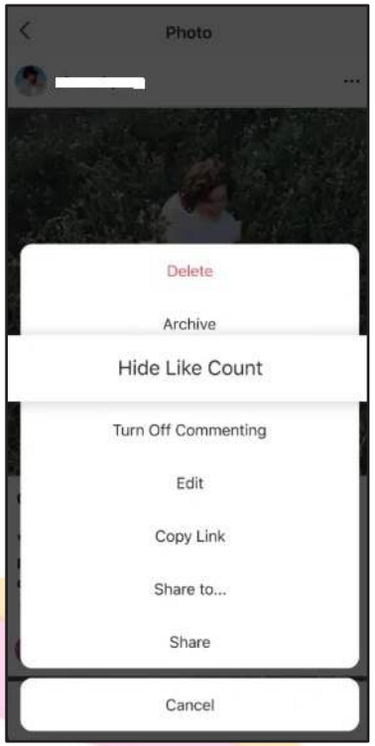
Following Influencers might seem like a strange step but it can help you stay with trends that your child might be exposed to. Don’t forget to keep the conversation going with your child and talk to them about what these influencers are doing and saying.

Foster realism

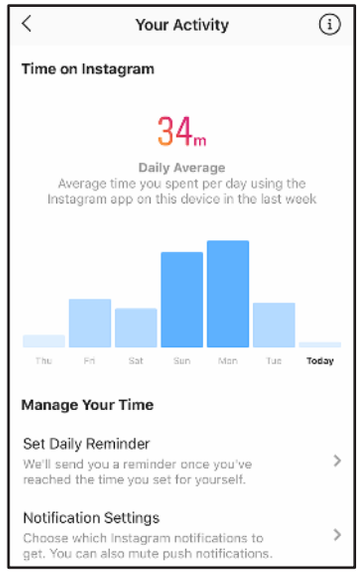
Filters are fun but they can be harmful. If a filter is being used to promote “beauty” then don’t be afraid to ask the child why they are using it and be aware of their self esteem. Do what you can to promote healthy expectations of themselves and to mark the difference of how people present themselves against how they probably are in real life.

Manage Like counting

Instagram allows users to turn off their Like counter through the notifications menu. This means that others will not be able to perceive the number of Likes on a specific post.
This feature was implement as a direct result of the Likes effecting the mental wellbeing of people



and it could be a good idea to take the focus off the popularity aspect of the App.



Take breaks

Instagram allows the use of an in-built activity dashboard which gives users the ability to see how long they have been on the App and even allows them to add a “Daily Reminder” to set a time limit on the App to keep them from losing too much time while scrolling. The dashboard also allows you to mute notifications for a while. Talk to your child about this feature and make sure they are aware of it and of the benefits of taking time away.

TikTok

TikTok (formerly known as Music. ly) is a social media platform for creating, sharing and discovering short videos. The app is used by young people as an outlet to

express themselves through singing, dancing, comedy, and lip-syncing, and allows users to create videos and share them across a community.

Age-innappropriate Content

Unfortunately due to the sheer amount of content uploaded to TikTok on a daily basis it is impossible to manually vet each one. For this reason, while the typical user of TikTiok will only see light hearted videos there is always a chance that a child’s “For You” selection could contain unsuitable content.

Dangerous Challenges

Children often imitate and unfortunately TikTok users often start Challenge Trends where a task is encouraged as the basis of a video or stream. Some are harmless but others have proven to be hurtful, illegal and in some cases have lead to the deaths of some users, including children.

Contact With Strangers

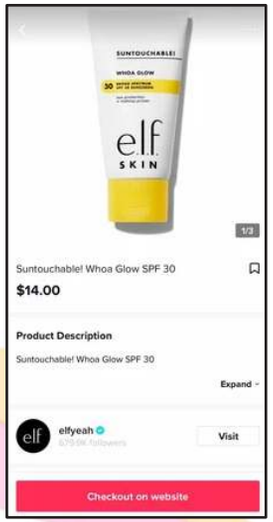
All accounts labeled as belonging to a person 16 years or older is or becomes public. Meaning that those who might be falsifying their age to seem older could be at real risk of encountering one of TikToks millions of users without supervision.

In-App Spending

TikTok allows users to purchase TikTok Coins that are used to purchase in App emojis which are then used to send to others. While some are relatively cheap others can be almost a hundred Euro. It is worth noting that while this feature is reserved for over 18's it can be accessed by falsifying ones age.

Addictive

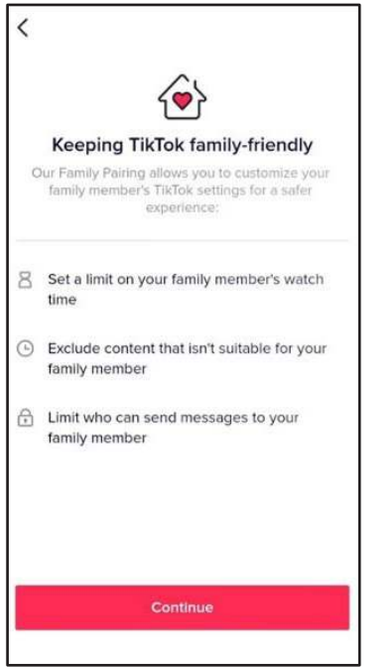
TikTok is designed to keep engagement going. It is part of the popularity of the platform. Each



pleasant ding and ring combines with the constantly engaging but short content keeps a lot of people coming back for more. This can obviously be a problem if it keeps people away from other activities and disrupts a regular sleeping schedule.

TikTok Now

This is a feature enables users to send a video or picture at the same time as a friend, much the same ass the app BeReal, which could be seen as a charming way of staying in touch but could result in private information such as a young users location being given away to those not intended to see it.



What can be done?

Use Family Pairing

TikTok has a Family Pairing feature which enables parents/guardians to link to a child's account and set certain parameters such as restricting the content possible to be viewed and setting a time limit on the amount of screen time allowed on the account.

Make An Account Private

While the age limitations for private accounts can be bypassed by falsifying ones age there is still a privacy setting tool that can be used to make an account unable to be viewed by anyone other than those on the users friend list. Restricting access to all content from that user.

Limit App Spending

Android and iPhone users can implement a 'Spend Limiter' on a TikTok account. So if your child is using such a device you can set up this limiter so that the child is unable to spend either past a certain limit or even at all. This is recommended for especially young users of TikTok.

Talk About The Dangers

Communication is key. If you allow your child to use TikTok then you should consider having a candid discussion with them about the potential risks that the platform may involve and stay informed about new features the platform provides.

Twitter/X

One of the leading social media platforms in the world 'X' is widely used by both professionals and private persons. You can post short messages, GIFs, Polls and even links to other sites all with the push of a button.

Paying for Verification

Unlike before it is now possible for anyone to purchase a verified account which means that anybody could potentially pose as a legitimate account holder. This has lead to impersonators effecting the reputation of both celebrities and brands.

Changes to Content Moderation

The new policy of X seems to be focused on limiting the reach of certain inflammatory content rather than limiting the use of it. This means that it still exists on the platform and as such it can end up being seen by young users.

Hashtag Mismanagement

Hashtags (#) have been one of the longest running features of X since its beginnings as Twitter. They were used to focus attention on a

specific topic. However any given Hashtag could get hijacked by any number of people for various purposes especially if it is popular and therefore people know that attaching their post to it will get it seen by a bigger audience regardless of the posts relation to the initial Hashtag.

Stranger Danger

By default all posts or "tweets" as they are called are public and able to be viewed by anyone. This presents the obvious risk that a child could be contacted by someone they do not know or find themselves interacting in the same circles as strangers. While this may simply be innocent enough there is always the possibility that someone could have alternative or even sinister motives.

View Count Watching

X has a feature that allows users to see how many times a Tweet or post has been viewed which has been found to lead to unfair comparisons with more famous users as well as insecurity and even jealousy among users.

Bullying

Because anyone can use a fake profile on X it is easy to send antagonistic and insulting tweets directed at people and groups without suffering any practical recourse for it. By inciting arguments for their own sake or slandering another user they can greatly effect the mental well-being of their targets as well as other users.

What can be done?

Use private settings on accounts

One of the easiest ways to keep a child safe is to use the privacy settings. By making a child's account private it means they must give approval before anyone can view their posts. You can also change the settings to make it so that the child cannot be contacted directly (PM'd or Private Messages) by other users. You can even keep their location from being displayed.

Get familiar with the updated Settings

Because of the transition between Twitter to X there have been some changes to the policy and settings. Get to know these changes yourself and you will be better able to educate your child on how they can keep themselves safer while using X.

Encourage Critical Thinking

Due to the nature of the platform it can be hard to know if what you are hearing or reading is the truth. Critical Thinking is the simple process of evaluating information against known facts and sourced material. By getting into the habit of checking sources early to verify facts a child will become more savvy about catching false information online and in general.

Take your time

Before you make a post, consider who might see it. Think about whether it contains any sensitive information such as the street you live on in a picture or if a link is to a video that might contain your home address. By being more careful and patient before posting you can encourage your child to do the same.

Turn on Safety Mode

Safety Mode is designed to monitor behaviour such as spam and repeated message that may contain hurtful or abusive language. It flags the culprit account and the platform can them block it. If they are Auto blocked then they cannot contact the blocking account (the child's account) for the next seven days.

Mute, Block and Report

If repeated harassment continues by an account you can use the Mute feature to censor tweets from specific accounts or even that contain certain word(such as slurs and swear words) from being seen by a child's account. Blocking will stop a blocked account from contacting the child's account and

Reporting will alert the platform to the abusive behaviour.

Don't follow everyone

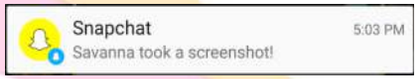
Since accounts have stopped being authenticated as thoroughly as they once were then people posing as celebrities or even people your child may know can appear overnight. Make sure your child is able to discern who they are in an effective way before deciding to follow them and always keep in touch with your child as to who they are currently following.

Snapchat

As one of the more famous photo sharing apps in the world Snapchat is used to share images and short videos. Which makes it a marvelous tool for staying in touch with quick messages over great distances. However it also has many features that are potentially harmful such as tracking user location, storing images and like all successful social media apps it is designed to promote frequent and repeated use

Location risks

The "Snap Map" feature shares your exact location with other users in real time. Allowing other users to know where your child is and what they may be doing. Even if they turn off the location settings if they upload an image or video to "Our Story" it will still turn up on the map if anyone searches the area for activity.



Lens Studio

The "Lens Studio" is a tool that enables any user to create a filter to use over their video or photo. Officially any Lens created by a user has to comply with the platforms Submission Guidelines (i.e. be suitable for any user 13 years or older) but that is not necessarily always the case. Meaning if a child using the "Lens Explorer" feature to browse potential filters they could come into contact with inappropriate material.

Recorded content and screenshots

One of the selling points of Snapchat is the idea that anything you post is temporary. Implying that it is relatively consequence free but while the platform may hide and store the images on its servers and not allow them to be seen by users it is still possible for any user to record the video they are watching and take a screenshot of an image. This means that anyone potentially could keep any photo or video they see without the initial poster's knowledge or consent.

Snap streaks and Addictive behavior

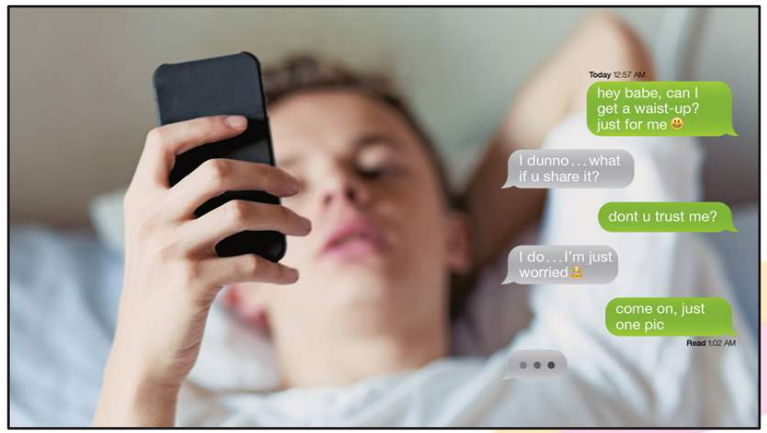
While all social media apps are designed to promote engagement it is always worth keeping in mind the potential for this to lead to addictive behavior. One way in which Snapchat encourages this is the use of its Snap streaks which rewards a consistent back and forth of messages between users. The reward system attached to this feature gives the users various emoji's and can put pressure on young people to carry on engaging when they should really stop.

Sexting

Snapchat is a unique platform which promises a lot of freedom, given the short lifespan of a message, and this has led it to be one of the chief go to platforms for Sexting as well as the sending of sexually explicit images to others. But this too can be screenshot and recorded which can lead to a great deal of issues including cyberbullying and blackmail. The storing, producing or reproducing of such images and videos involving a person under the age of 18 is illegal in The Republic as well as Northern Ireland. Even if the image or video has been created by the person under 18 in question it is still illegal.

Snap Originals

"Snap Originals" is another feature designed to promote engagement by allowing users to watch Snapchat created content such as shows, comedy sketches, news reports etc. Like other features this can encourage addictive behaviour in users.



What can be done?

Talk about the risks of Sexting

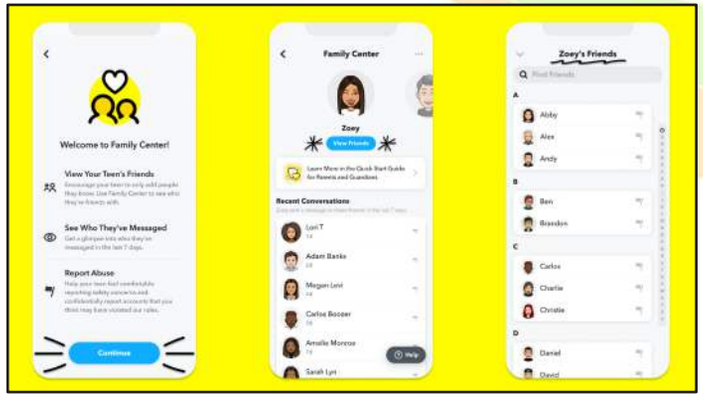
While it will undoubtedly be awkward to bring up this topic with your child it can be well worth it to educate them in order to help keep them safe. Make certain that they are aware of the risks involved (including blackmail, embarrassment, cyberbullying, fraud). Let them know that by screenshots and recordings of their content can be kept essentially forever by anyone who happens to see it and that they could be shared with anyone at any time.

Report unsuitable material

Advise your child to report any material that is inappropriate, including threatening or sexually suggestive ones. Inform them how to report on messages, videos and lenses. Lens report function can be in the info button that appears when a lens is selected.

“Ghost Mode”

You can activate Ghost Mode by opening Snap Map, tapping the cog in the top-right corner and from there change the setting to “Ghost Mode”.
Ghost Mode means your child will no longer visible on the Snap Map. However their history may still be accessed to see where they have been in the last 24 hours.



Know how to Delete a message

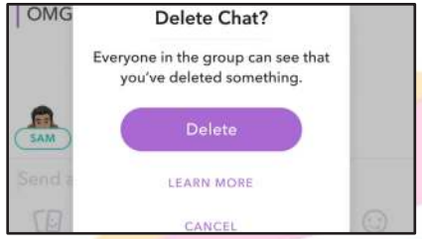
A message can be deleted by pressing and holding the message then the option to delete it will appear. Advise the child to record and screenshot any offensive and abusive behaviour they have seen directed at them. This record can be used to report inappropriate behaviour.

Disable “Quick Add”

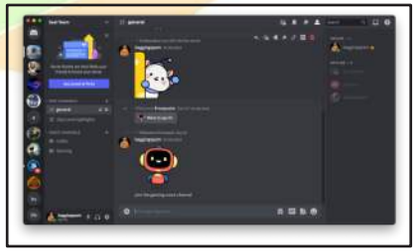
It is recommended that your child turn off the “Quick Add” feature in their settings. “Quick Add” allows a user to find others based on mutual friends. This is handy in one way but also opens up young users to strangers and it is important that they understand the risks involved in this. Talk to your child about what this could mean and that they are not to assume that mutual friends means they will or have to be friends with these people.

Control who can view your Story

Snapchat’s settings by default allow anyone in a user’s friend list to view their posts but this setting is subject to change by the Platform so it is recommended that you stay familiar with the privacy settings and check regularly who can see your Story. The Settings menu has a section for this labelled “Who can see my Story” where you can manually edit this setting.



Discord



Discord is a free to use app that was initially designed to allow gamers to quickly communicate while playing but has become a more generalized platform for all manner of topics including books, music and TV shows. You can make a server about any topic you wish, small or large. But such accessibility can pose dangers to the unwary and as always young children are some of those most at risk.

Cyberbullying

Because it is so easy to use and access it means that it is also a place that can allow cyberbullying to happen very easily. Besides messages audio channels can allow people to get verbally abusive and because there is no recording function it means no evidence of verbal abuse can be left. The prime feature being the ability to create independent groups, while attractive can mean young people are locked into area where abuse can flourish.

Moderation Difficulties

Like all apps that let you send instant messages Discord is difficult to moderate as it happens. As a rule, each server can select its own Moderators and decide amongst the users what the individual rules are for that server but this creates the obvious issue of stumbling onto unsuitable content.

Inappropriate Content

Because individual servers create their own rules it means there is always the possibility that any server a child or young person joins could be host to racism, sexism, pornography or extremely violent imagery and videos. Despite the rule that Servers hosting such things need to be designated as strictly 18+ with an age-restriction gate the lack of user age verification means this can be bypassed at times.

Predator Activity

As with all chat platforms it is easy enough to falsify your name and age. This means that Predators can abuse the platform in order to engage with younger and vulnerable people even going so far as to establish themselves in an age appropriate server first. While Discord has taken steps to close this weakness in its system it is still vulnerable.

Criminal Activity

Despite the very strict Terms of Service and Community Guidelines criminal activity is still an issue. Hate speech, grooming and harassment of various kinds have all been found on Discord Servers. While Moderation happens it is not able to catch everything and once found it is easy to start a new account and make a whole new server to host illegal activity.

What can be done?

Familiarise yourself with the safety settings

Like with all social platforms Discord has safety settings. Learning how to operate these settings and teaching your child how to operate them so that they

have to tools they may need to keep their presence as private as possible.

Keep an eye out

Talk to your child about their online activity using Discord. Go over which servers they are using and ask them about the people there. Don't be afraid to ask about how the server makes them feel and if they have any concerns about it or any messages they have received.

Explaining the age filter

Let your child know that Age Filters exist for a reason and that accessing an age restricted server means they could see upsetting or adult intended content (often labelled NSFW or Not Safe For Work). That is why the filter exists and that it is there for the sake of the child.

Be practical about good online behaviour

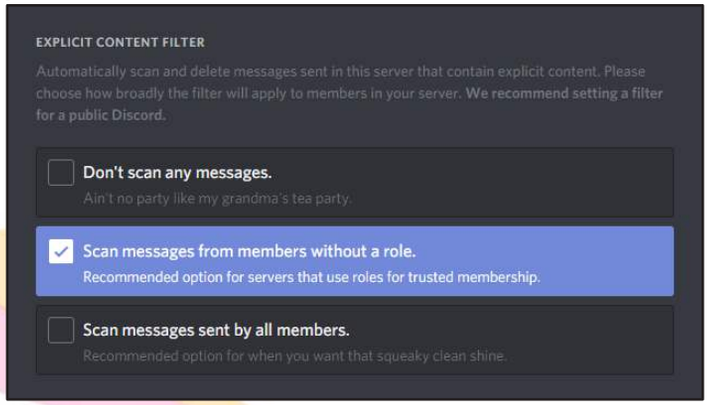
Explaining to your child that even though users are anonymous that they do deserve respect and consideration is a vital step in helping them to create a respectful and mature online presence. Beginning these practices early is a great way to get them to continue with it at later stages.

Enable content filter

While a lot of explicit images will automatically be censored the same is not default for written messages. That feature has to be enabled through the settings menu. It will target and delete messages coming in that contain explicit material.

Be open and honest

It is never easy to have the frank conversations you may need to with your child about internet safety and the dangers they could be faced with but it is a conversation worth having. Your child should be aware of these dangers so that they know what to come to you with and are prepared to take the best action possible.

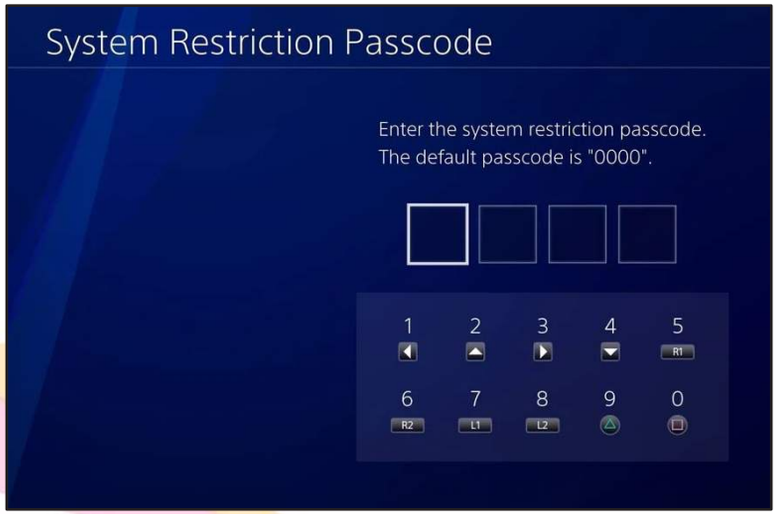


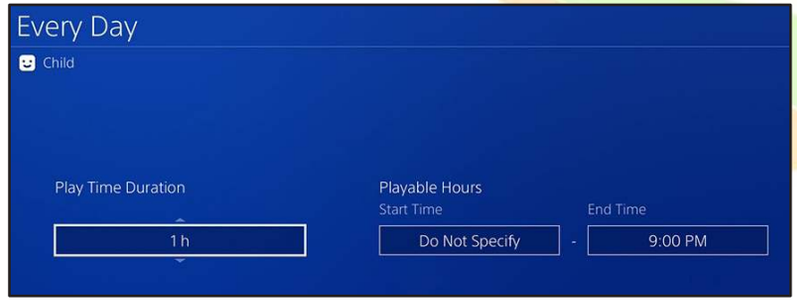
Consoles

PlayStation 4

Like other devices connected to the Internet it's important to ensure that your child is safe while using their PlayStation. One way to do this is by setting up parental controls on the console. Here's a guide to help you set up these controls and keep your child safe:

1. Setting up a passcode: Set up a passcode that only you know. This passcode will prevent your child from changing the parental control settings without your permission.
2. Age restrictions: You can set age restrictions for games, movies, and TV shows based on your child's age. This will prevent them from accessing content that is not appropriate for their age.
3. Time restrictions: You can also set time restrictions on how long your child can play games or use the console. This





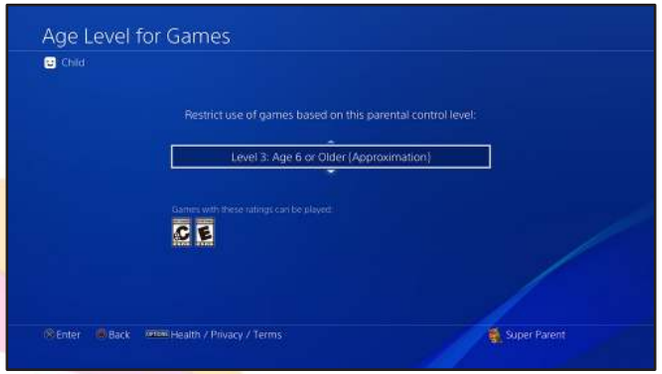
will help ensure that they don't spend too much time playing games and neglect their other responsibilities.
4. Communication and social features: You can disable communication and social features to prevent your child from interacting with strangers online.
5. Web browsing: You can also disable web browsing to prevent your child from accessing inappropriate content on the internet.
By setting up these parental controls, you can ensure that your child is safe while using their PlayStation. Remember to regularly review and update the settings as your child grows and their needs change.

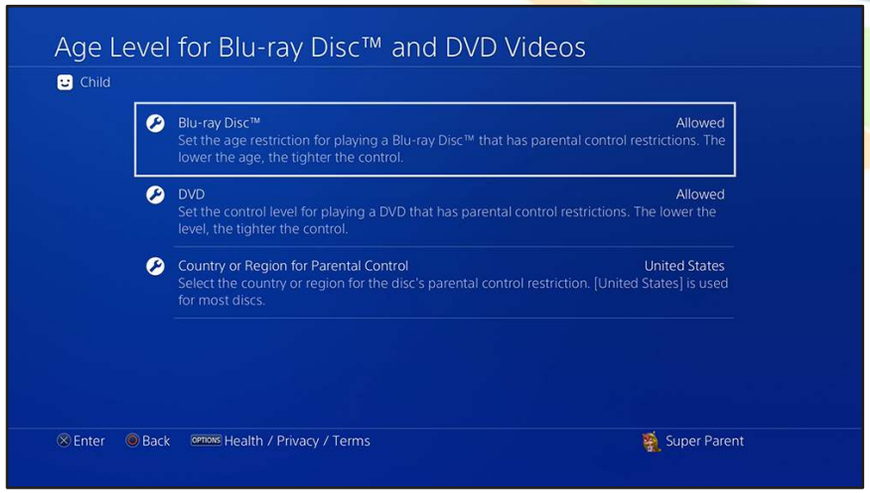
A parental guide to setting up parental controls on the PlayStation

It can be a challenge to ensure that your child's gaming habits are healthy and safe. One of the ways the PlayStation can help you with this is by setting up parental controls on the child's console.

1. To begin, you'll need to create a separate user account for your child. This will allow you to apply specific settings and restrictions to their account.

2. Once you've created the account, navigate to "Settings" and select "Parental Controls/ Family Management."
3. From here, you can set age restrictions for games, limit access to online features, and even set a time limit for gaming sessions.
Another important feature is the ability to restrict access to certain types of content, such as movies and TV shows. You can also disable the ability to make purchases within the PlayStation Store.





It's important to remember that parental controls are not foolproof, and it's always a good idea to monitor your child's gaming habits and have open communication about responsible

gaming. By setting up these controls, you're taking an important step in ensuring that your child is safe and healthy while enjoying their PS4.

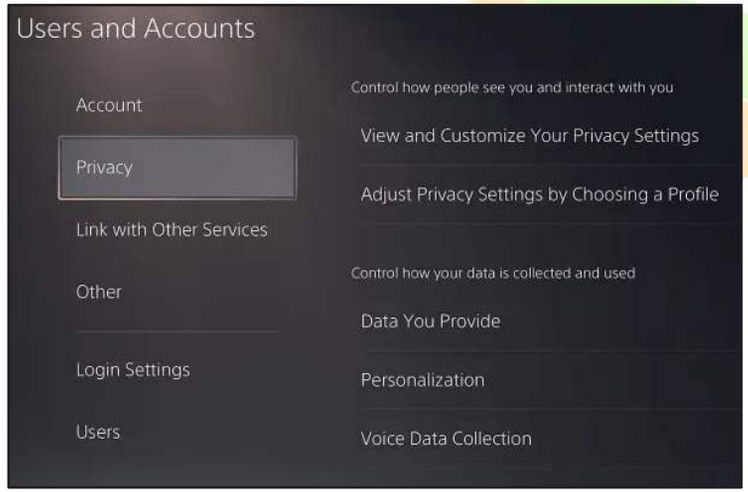
PlayStation 5

As a parent, you may be concerned about the content that your child can access on their PlayStation 5. Fortunately, the PS5 has some built-in parental controls that can help you manage your child's gaming experience. In this guide, we will go over how to set up parental controls on the PS5.

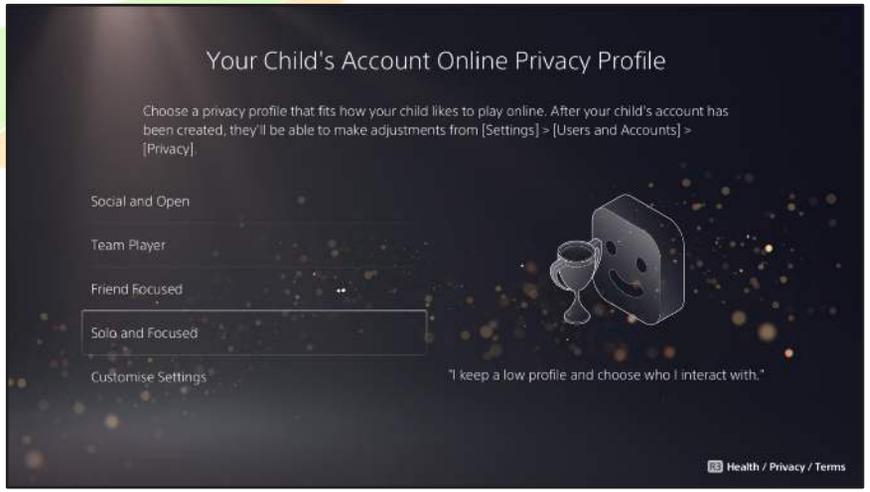
First, you will need to create a sub-account for your child.

One of the most important settings is the age rating for games. You can set the maximum age rating for games that your child can play, and any games with a higher age rating will require a parental control password to be played. You can also set restrictions on online communication, so your child can only communicate with friends that you have approved.

Another useful feature is the Play Time Management setting, which allows you to set daily playtime limits for your child. Once the limit has been reached, the PS5 will automatically log your child out of their account.



It is highly recommended that you as Parent/Guardian take the time to get familiar with these settings so that you can use them effectively. Overall, the PS5's parental controls are a useful tool for managing your child's gaming experience. By setting up restrictions on age ratings, online communication, and playtime limits, you can ensure that your child stays safe while playing their favourite games.



A parental guide to setup and privacy settings for PlayStation 5

As a parent, it is important to ensure that your child is safe while using their PlayStation 5.

Here is a guide to setting up and adjusting privacy settings on the PlayStation 5:

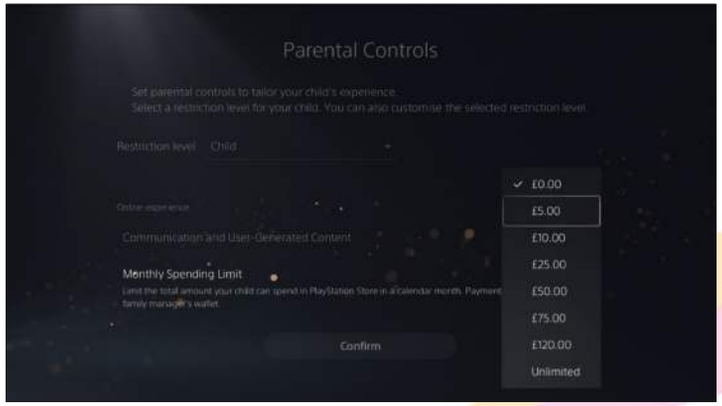
1. Setting up a Child Account
To ensure that your child is using an age-appropriate account, set up a child

account for them. You can do this by going to Settings > Family and Parental Controls > Family Management > Add Family Member. From here, you can add a child account and set restrictions based on their age.

2. Adjusting Privacy Settings
To adjust privacy settings, go to Settings > Users and Accounts > Privacy. Here, you can adjust settings such as who can see your child's online status, who can send them friend requests, and who can see their real name.

3. Enabling Parental Controls
To enable parental controls, go to Settings > Family and Parental Controls> Family Management. From here, you can set restrictions on game content, set time limits for gameplay, and restrict access to certain features such as online communication.

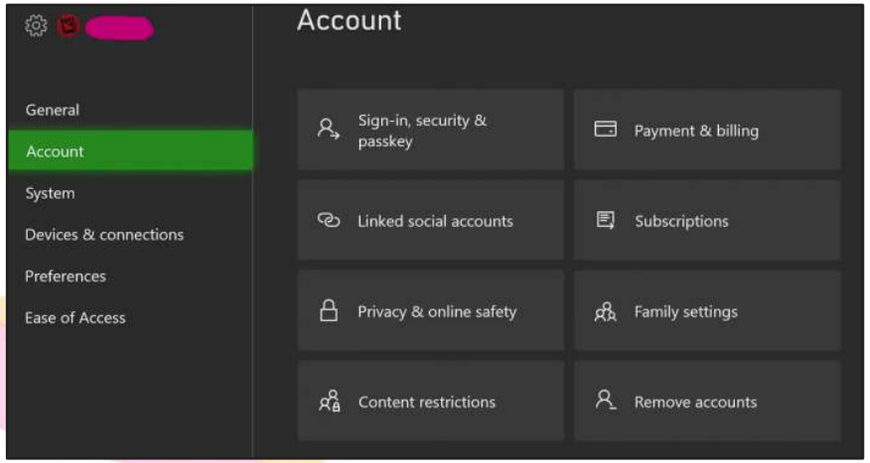
By following these steps, you can ensure that your child is safe while using their PlayStation 5. Remember to regularly check and adjust settings as needed to ensure their continued safety.

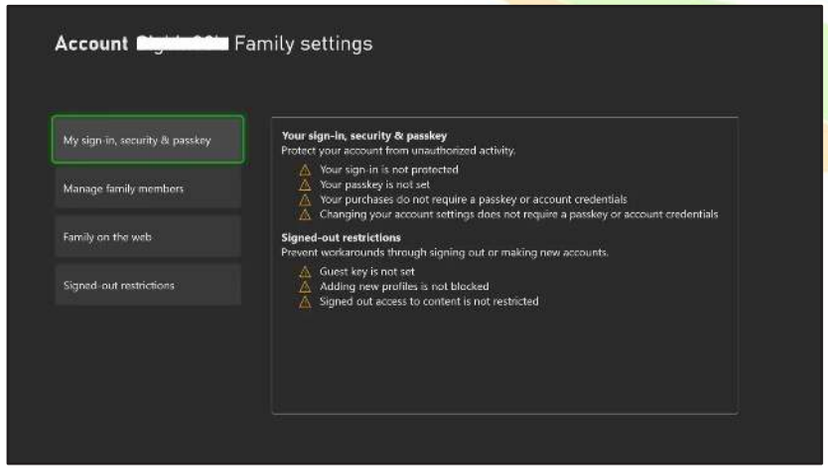


Xbox One S/X

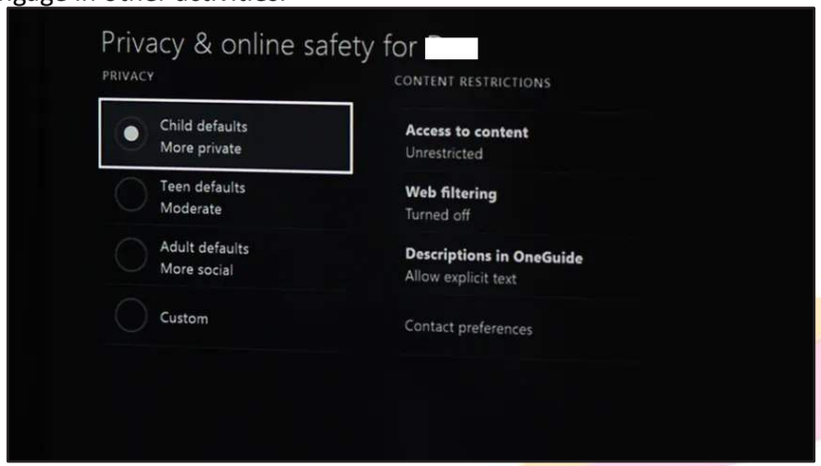
Xbox One is a popular gaming console that offers a wide range of games and entertainment options. However, as a parent or guardian, you may be concerned about the content your child is exposed to while using the console. Fortunately, Xbox One offers several parental control features that can help you regulate your child's access to content.

To set up parental controls on Xbox One, start by creating a child account for your child. You can then customise the account's settings to control the content your child can access. For example, you can set age restrictions for games, limit access to online content, and restrict purchases.





You can also set up screen time limits to ensure that your child is not spending too much time playing games or watching videos on the console. Xbox One allows you to set up daily and weekly time limits, and you can also set up breaks to encourage your child to take a reak from the screen and engage in other activities.

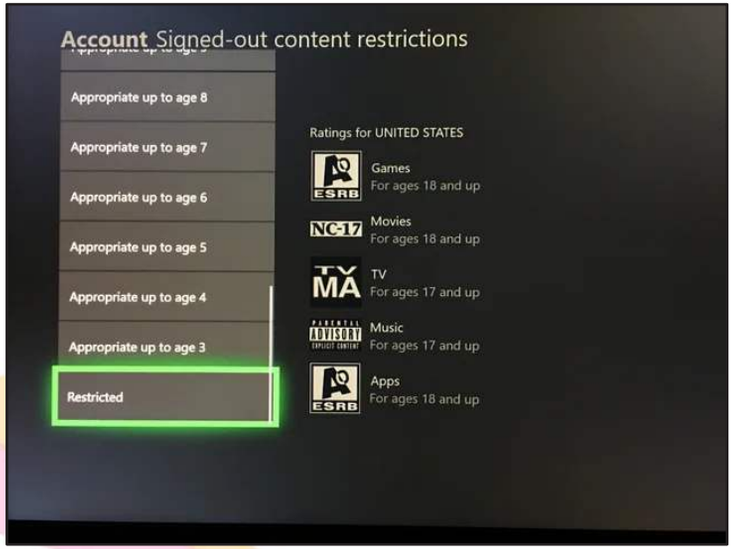


Another useful parental control feature on Xbox One is the ability to view activity reports. These reports can show you how much time your child is spending on the console, the games they are playing, and the websites they are accessing. By reviewing these reports regularly, you can monitor your child's activity and ensure that they are using the console safely and responsibly.

Overall, setting up parental controls on Xbox One is a simple and effective way to regulate your child's access to content. By taking advantage of these features, you can encourage safe and responsible use of the console while still allowing your child to enjoy all the entertainment options it has to offer.

Setup guide for parental controls for the Xbox One

The Xbox One is still used by many individuals and families, so it is normal to be concerned about the content your child is exposed to while using the Xbox One.



Thankfully, the Xbox One has built-in parental controls that allow you to restrict access to certain games and apps, limit screen time, and monitor your child's activity.

To set up parental controls on your Xbox One, follow these steps:

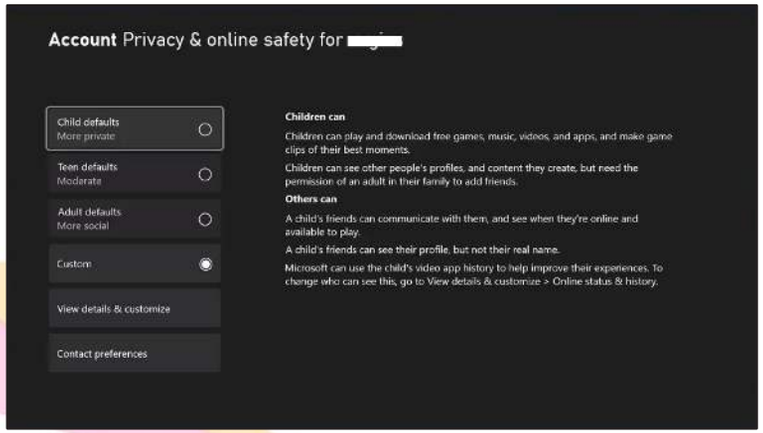
1. Press the Xbox button on your controller to open the guide.
2. Select ‘System’ and then ‘Settings’.
3. Select ‘Account’ and then ‘Family’.
4. Enter Password or Passkey to proceed.
5. Choose the account you want to apply the parental controls to.
6. Select ‘Privacy & online safety’ and then choose the default settings or customise by selecting ‘View details & customise’.

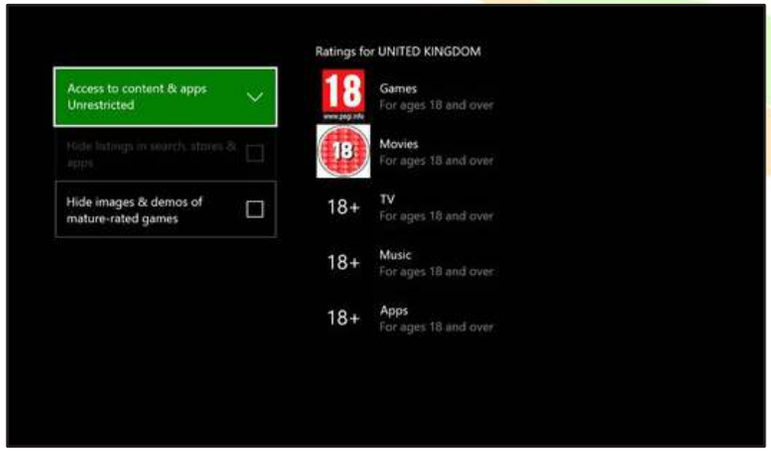
Additionally, you can download the Xbox Family Settings app on your smartphone to manage your child's activity on the Xbox One remotely. With the app, you can approve or deny requests for additional screen time, view your child's activity history, and adjust settings as needed. By setting up parental controls on your Xbox One, you can ensure your child is only exposed to age-appropriate content and limit their screen time for a healthy balance of gaming and other activities.

Xbox Series S/X

The Xbox Series S and X has a variety of parental settings that can help parents manage the content their children are accessing on the system. One of the most useful settings is the ability to create child accounts, which can be customised with specific permissions and restrictions. Parents can also set limits on screen time, block specific websites and apps, and even restrict certain types of content based on age ratings.

Additionally, the Xbox Series X has a feature called 'Ask a parent,' which requires parental permission before a child can make any purchases or access certain content. Overall, the parental settings on the Xbox Series X provide a range of options for parents to ensure their children are using the system in a safe and appropriate manner.

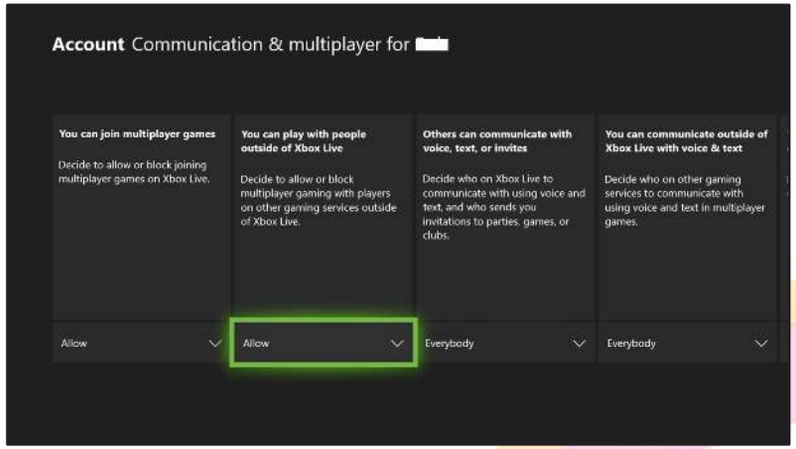




Xbox series X parental settings setup instructions

If you're a parent who wants to ensure that your child can safely play on the

new Xbox Series S or X, there are several parental settings you can set up to limit what your child can access.



Here's a step-by-step guide to setting up parental controls:

1. Sign in to your Xbox Series X with your Microsoft account.
2. Press the Xbox button on your controller to open the guide, then select Profile & system > Settings > Account > Family settings.
3. Select the child account you want to manage, then select Manage family members.
4. Choose the child's account you want to set up parental controls for, then select Privacy & online safety.
5. Here you can set up various settings to restrict what your child can access, including:

- Content restrictions: You can choose to block explicit content and set age limits for games, movies, and TV shows.
- Communication & multiplayer: You can choose to block your child from communicating with other players and from playing multiplayer games.
- App and game limits: You can set time limits for how long your child can play games and use apps each day.
- Web filtering: You can choose to block inappropriate websites and set up a list of approved websites.

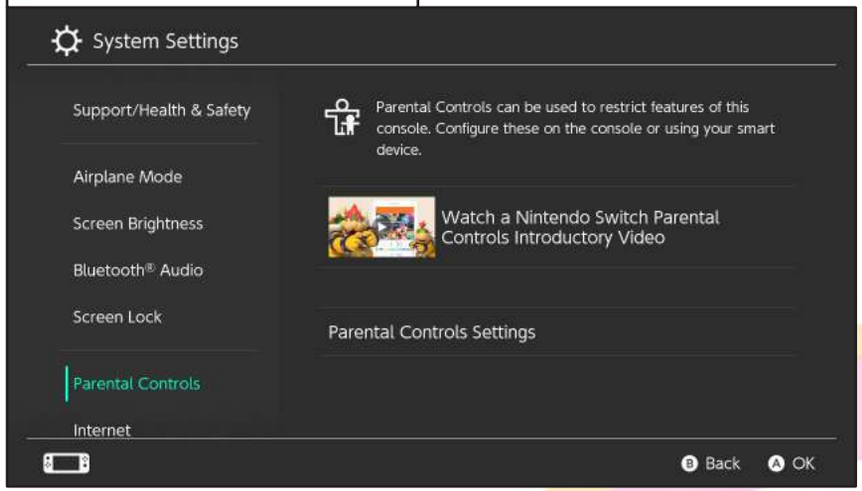
6. Once you've set up the desired parental controls, select Save to apply the changes.

By following these simple steps, you can ensure that your child can play on the Xbox Series X safely and with age-appropriate content.

Nintendo Switch

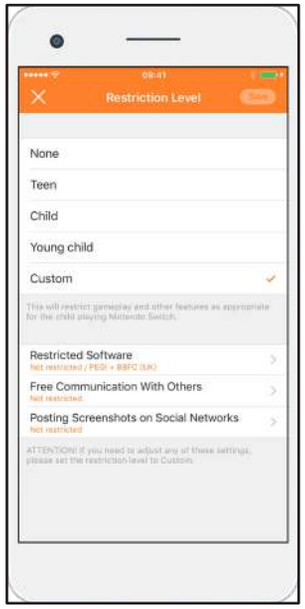
The Nintendo Switch is a popular gaming console that is suitable for children and adults alike. As a parent, it is essential to understand the features and capabilities of the Switch to ensure that your child is using it safely and responsibly. Here are some tips to help you navigate the Nintendo Switch:

1. Set parental controls: The Nintendo Switch has built-in parental controls that allow you to restrict access to certain features. You can set limits on gameplay time, restrict access to certain games, and even block access to the internet browser. To set up parental controls, go to the System Settings and select Parental Controls.

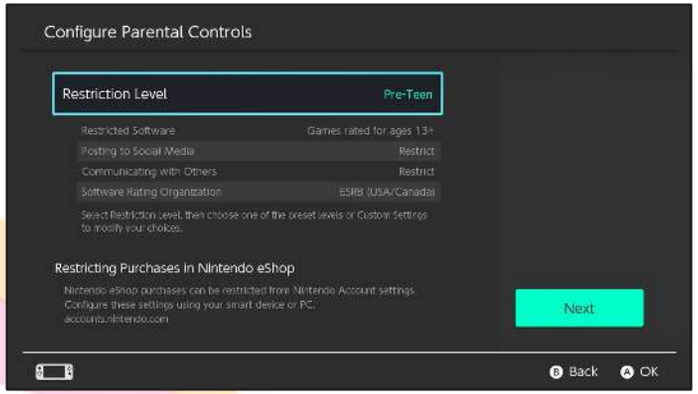


2. Choose age-appropriate games: The Nintendo Switch has a wide variety of games available, but not all of them may be suitable for your child. Be sure to check the game's age and content rating before purchasing it. The Entertainment Software Rating Board (ESRB) rates games based on age appropriateness and content.

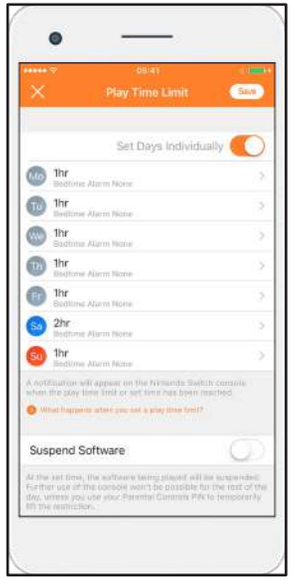
3. Monitor online activity: The Nintendo Switch allows for online play, which means your child may be interacting with other players online. Be sure to monitor their online activity and ensure they are not giving out personal information or engaging in inappropriate behaviour.



4. Use the Switch's handheld mode: The Nintendo Switch can be played on a TV or in handheld mode. Using the handheld mode allows you to monitor your child's gameplay more closely and limit their exposure to screen time.



5. Encourage breaks: Playing video games for extended periods can lead to eye strain and fatigue. Encourage your child to take breaks and engage in other activities to prevent overuse.



Overall, the Nintendo Switch can be a fun and safe gaming console for children when used responsibly. By setting parental controls, choosing age-appropriate games, monitoring online activity, using the handheld mode, and encouraging breaks, you can help ensure your child's gaming experience is both enjoyable and safe.

Parental Control setup for Nintendo Switch Console

As a parent you may want to limit your children's access to certain games or features. Luckily, the Nintendo Switch has a built-in Parental Controls feature

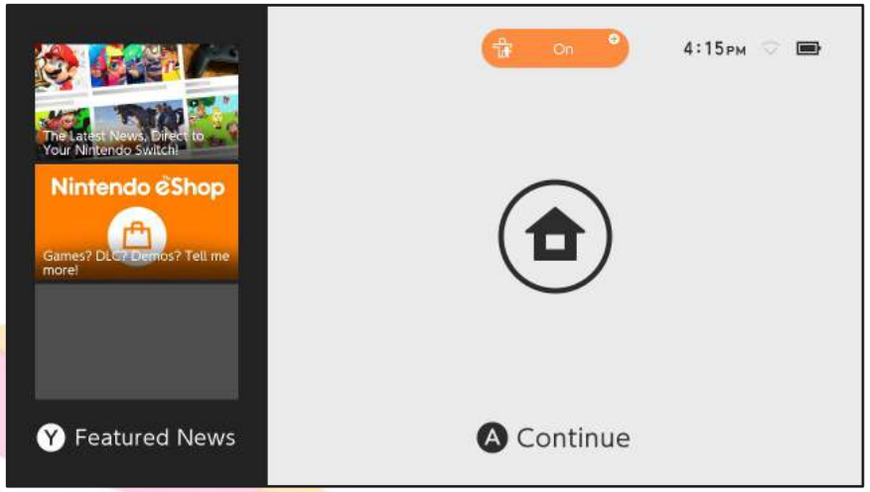
that allows parents to set restrictions and monitor their children' gaming activity. Here's how to set it up:

1. Go to the System Settings on your Switch and select "Parental Controls" from the menu.
2. Choose "Use this console" to set up the controls.
3. From there, you can set restrictions on games based on their content rating, limit online communication and social media features, and even set time limits for gaming sessions.
4. Follow the prompts to set up a PIN (Between 4 to 8 digits long) and create a profile for your child.

Setting up Parental Controls on your Nintendo Switch can help ensure that your child is only playing age-appropriate games and staying safe online. It's a simple process that can provide peace of mind for parents.

Parental Control on smart device setup for Nintendo Switch Console

Setting up a smart device to the Nintendo switch can be a good way to monitor your child's gaming activity, a simple way to set it up is the followed:



1. Ensure you have linked your Nintendo Switch console to the Parental Controls application afterwards you will need to start the application.
2. Select Settings in the upper-right corner (Android) or lower-right corner (IOS), If it's your first time opening the app there will be a walk through for the different settings.
3. Select and customise the different settings you wish, Important to note is the Eshop including the restriction of spending/purchases much be set in the Nintendo Account Settings.
4. You can set a play time limit and also add a restriction level based of the age of the child and even whitelist certain applications (Allows play and use without needing the Parental PIN).
5. You can view or change the parental Controls pin on the Application.

The Smart device linked to the Nintendo Switch will help you monitor and edit any restrictions you wish to have so your child can have a fun and safe time.

How to remove Parental Controls on the Nintendo Switch

If the time comes where you wish to remove the Parental Control on the console, Here's a quick few steps to help free it of any restrictions that you have implicated.

1. Go to the "System Settings" on the HOME menu.
2. Select "Parental Controls" and then follow up with the "Change Settings"
3. You will be required to input the PIN that was selected when first set up.
4. You can press "X" to "Delete Settings" and it should remove the parental Controls and PIN

Afterwards your console should be restriction free and the Parental Control should be gone until set back up again.

Notes

Notes

Eolas Don Ógra

YOUTH INFORMATION

For more information on any topics raised in this booklet, please contact us at Donegal Youth Service on:

(074) 912 9630

Or visit us at

16 - 18 Port Road,

Letterkenny,

Co. Donegal

This project was led by Donegal Youth Service supported by CYPSC Seed funding from Dept. Of Children, Equality, Disability, Integration and Youth

CYPSC
CHILDREN & YOUNG PEOPLE'S SERVICES COMMITTEES
Donegal

TUSLA
An Ghníomhaireacht um Leanaí agus an Teaghlach
Child and Family Agency

An Roinn Leanaí, Comhionannais, Míchumais, Lánpháirtíochta agus Óige
Department of Children, Equality, Disability, Integration and Youth

Donegal Youth Service
Youth Work Ireland