Parenting in the Digital World:

Keeping your child safe online

Together we can

Foreword

Connectivity brings many benefits, and deciding when your child is ready to go online on their own device can be difficult.

Vodafone Ireland fully supports the decisions of parents/guardians as to if and when their child should have their own smartphone or device, including the voluntary agreements made by parents in some primary school communities.

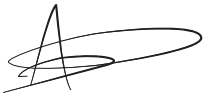
Safeguards are needed to protect children online. To help parents/guardians to understand the safety and control settings available on devices, we've made information and how-to guides such as this one available on our website and in store.

Our unique SecureNet option also gives an extra layer of oversight, limiting time online and blocking certain websites and apps on our network.

If you want to be able to contact your child without giving them full internet access, our basic phones with limited 2G data functionality (no internet access or social media apps) could be a good option for you.

The Vodafone Foundation is investing €3 million in Tozi, an app designed by the Dublin City University Anti-Bullying Centre to support young people aged 11-14 in guarding their wellbeing online. Tozi is free and available to everyone, not just Vodafone customers.

We believe in the positive power of connectivity and hope that this guide supports you in protecting and supporting your child, ensuring they enjoy good digital experiences and habits.



Amanda Nelson
CEO, Vodafone Ireland

Parents' Checklist

- [ ] Think about why your child wants or needs a phone.
- [ ] Decide when to give your child a device. Don't allow it to be given as a surprise gift or hand-me-down.
- [ ] Talk to your child about getting a phone.
- [ ] Decide what you want your child to do with their phone.
- [ ] Check if their school has a no-phone policy.
- [ ] Consider if your child can manage their time or do they get too focused on one thing?
- [ ] Use parental controls.

Parents' Checklist

If you feel like your child isn't ready for a phone, talk to them openly about why they want one and the responsibilities that come with it. Explain that while their friends might have phones, every family makes decisions based on what's best for them.

Encourage them to share their feelings and remind them that not having a phone doesn't mean they are missing out. Suggest other ways to stay connected with friends and stress the importance of waiting until they can handle all that comes with a device. Helping your child feel confident in making their own choices can make it easier for them to handle peer pressure and make the best decision for themselves.

Only you can know when your child is ready to have a phone or tablet with internet access. Just as you put them in a child seat in the car, reminded them to wear a helmet on their scooters and bikes, it is up to you to use all the safety measures available to you to protect your child online. In making that decision, make sure you know about – and how to use – all the control settings that are available to you, such as Secure Net, or your child's device control settings which will be outlined in the device guidebook. All devices have their own individual safety features which can limit the time spent online, prevent access to certain apps and monitor usage. When you are setting up a device for your child, consult with the manufacturer's device guide to ensure you choose the most suitable device safety settings to keep your child safe online. Another useful parental app is the Google Family Link app which is available for free for Android devices.

Digital Resilience

What is Digital Resilience?

Digital resilience is knowing how to get help and recover after an upsetting experience online. Building your child's digital resilience is one way to help them cope if something negative does happen.

How can I build my child's digital resilience?

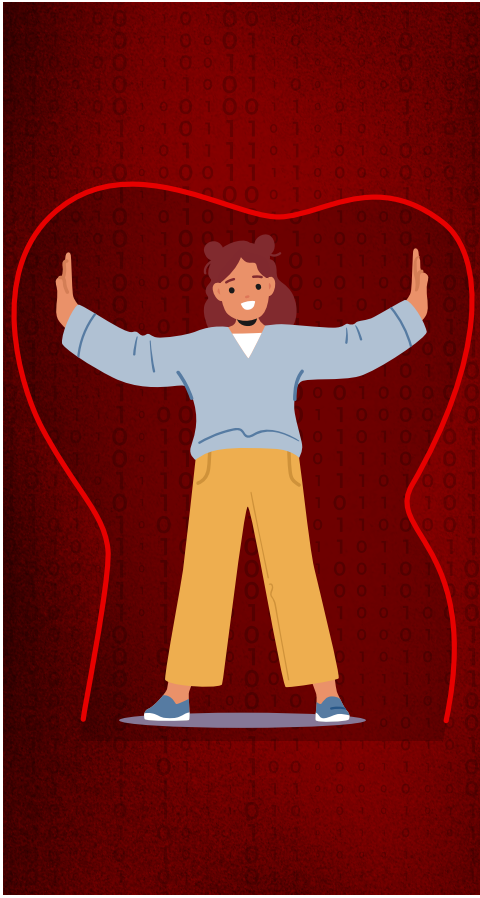
Start by talking openly to your child about the risks and types of content they might come across online. Explain that safeguards like parental controls are there to protect them, not to limit their fun. Having open conversations helps your child feel comfortable coming to you with any issues and makes sure they feel safe and supported while using the internet.

SET BOUNDARIES

Before your child is given any device, agree on some ground rules together. These could include limits on what they use it for, or where, when and how long they use it. You'll have your own views on this, but it can be helpful to ask your child for their take too. When your child feels listened to they might come up with reasonable suggestions for their own usage. Respecting their experiences also helps to build trust and openness between you.

Here are some questions you could ask:

- Why are you going online? (Helps to focus them and avoid endless hours scrolling)
- How do you know when it's time to switch off?
- How do you feel when you spend too much time in front of a screen?



Building a positive offline world is also key – the internet is a great resource, but it shouldn't replace real life interactions. Fresh air, regular exercise, and good sleep are crucial to a child's development as they promote physical health, mental well-being, and optimal cognitive growth, laying a strong foundation for lifelong habits.

TALK, TALK, TALK

Remind your child that you are always there to support them. Make sure your child knows they can talk to you about anything they see online and that you'll be there to help them if something does go wrong. Let your child know that they won't get in trouble if they ask for help.

While you might be aware of a younger child's usage through parental controls, for older teenagers, open communication is vital to understand their behaviour online. Try not to be too judgemental when your child tells you how much time they spend on their devices. It's okay to be concerned, but a strong reaction could stop them from talking to you about it again.

Discuss the risks of posting and sharing photos of themselves online or through messaging apps. These images can easily be shared or forwarded. Remind your child that the internet doesn't have a 'Delete' button and what they post online can be very difficult to remove.

USE THE TECH

Download the Tozi app

Tozi helps children understand the impact their digital lives may be having on their mental wellbeing. The Vodafone Foundation has partnered with Dublin City University's Anti-Bullying Centre and the ISPCC to develop Tozi, a first-of-its-kind app that offers support for children and young people by educating them on how to be safe and well online, while offering instant support if they need it. The Tozi app is available for free download and usage from the Google Play Store and Apple App Store.

Download Vodafone Secure Net app

When you first set up your child's device, make sure to use useful parental controls tools such as the Vodafone Secure Net app* which has a range of settings to help parents manage their child's device usage. The app is available from the Google Play Store and Apple App Store and protects devices from viruses, dangerous files and harmful websites when you're using the Vodafone network – on mobile and on broadband at home. It analyses your network traffic, blocking harmful or unsafe downloads, and alerting you of the download via SMS. It also gives you the following parental control features so that you can easily manage usage and access on your family's internet:

- Content Filtering
- Pause your Wi-Fi
- Bedtime
- Focus Time

More information on the Vodafone Secure Net App is available on www.vodafone.ie or you can talk to one of our customer advisors in any Vodafone store nationwide.

* The Vodafone Secure Net App is for Vodafone customers only. Requires subscription.

Online Risks and Cyberbullying

No parent or guardian wants to imagine their child is being bullied or harassed online. Sadly, cyberbullying is happening which means you need to make yourself aware of some of the forms it can take. These include:

Peer Pressure

Using a public online platform to pressure someone into taking part in something they don't want to do (like an online challenge) or forcing them to reveal information.

Social Exclusion

Social exclusion is when your child is excluded from a friend WhatsApp group or discovers that a group was set up specifically to talk about them with the members sharing mean comments. Friends posting group pictures online without your child with the intention of causing upset is another example.

Nasty DMs

Even if there are no obvious problems on your child's public social media feed, they might be getting nasty or hurtful private messages in their Direct Messages (DMs). Certain apps such as Snapchat will make messages disappear after 24 hours, so it is important to be aware of this.

Image-Based Bullying

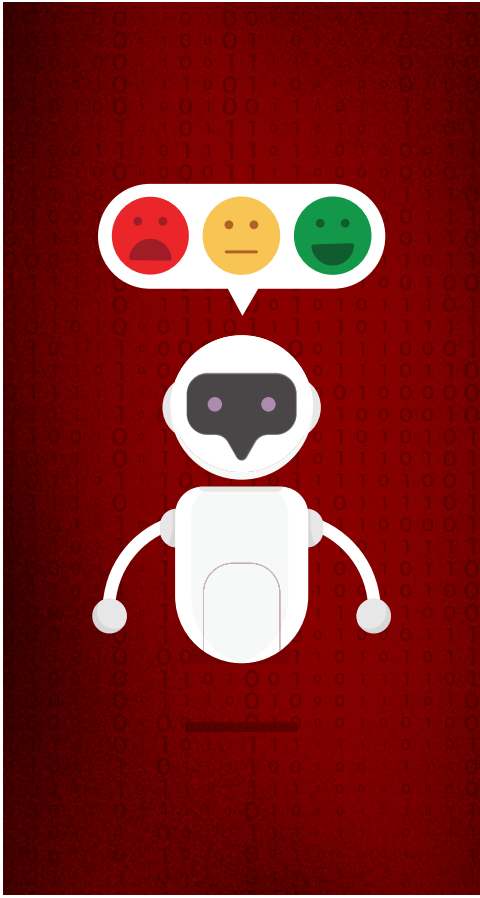
Even if it's meant 'as a bit of fun,' sharing embarrassing or compromising images of someone can really hurt a young person's feelings and self-esteem. There are now laws to protect people from the sharing of intimate images, which can result in prison sentences from one to seven years, as well as fines. However, even if the person who shares the image gets in trouble, the person in the picture is still affected. It's important to talk to children about these risks so they understand the impact of sharing images of themselves or others online, including facing the serious consequences of breaking the law.

Fake Accounts

Cyberbullies might set up a fake account specifically to send unkind messages or spread lies. These can be blocked and reported to the social media platform but are tricky to manage as there are few safeguards in place to stop the person from setting up new ones.

Trolling

Trolling involves targeting people and/or groups, challenging their viewpoints and trying to provoke a reaction in them, or others to turn against them, sometimes leading to the victim(s) shutting down their social media account as they no longer feel able to participate safely.



What you can do

What can I do if my child is a victim of cyberbullying?

STAY CALM

Try not to overreact. When first talking to your child, focus on listening and taking the time to think through the next steps. While it's understandable that you might feel anxious, it's important that your child sees you as a calming force in a crisis. Talk to your child about what they would like to see happen next and how much help they want. You might be tempted to take their computer or phone away - to put a stop to the bullying - but your child might see this as being punished for being bullied and put them off coming to you in future.

USE THE SUPPORTS

The ISPCC has a support line for parents where you can chat to a therapeutic support worker for support or advice. Open Monday – Friday, 9am -1pm on 01 522 4300. The Tozi app (outlined in section 1) was designed to create a safe space for your child online.

SAVE ANY MESSAGES AS EVIDENCE

Where possible, keep track of the details, dates and times of any form of harassment that your child experiences. This will be very useful should there be a subsequent Garda investigation.

DELETE THE APP

It may be appropriate in some instances to delete the app where the incident occurred (but remember to save evidence beforehand).

ADVISE YOUR CHILD NOT TO RETALIATE

Bullies are looking for a strong reaction and response from their target. Instead, block them. Every site has a way of blocking and reporting.

CONTACT AN GARDA SÍOCHÁNA

Go to your local garda station if the abuse is particularly threatening or serious. Please note that Hotline.ie is the Irish national reporting centre where members of the public can securely, anonymously and confidentially report suspected illegal content online, especially child sexual abuse content and activities relating to online child sexual exploitation.

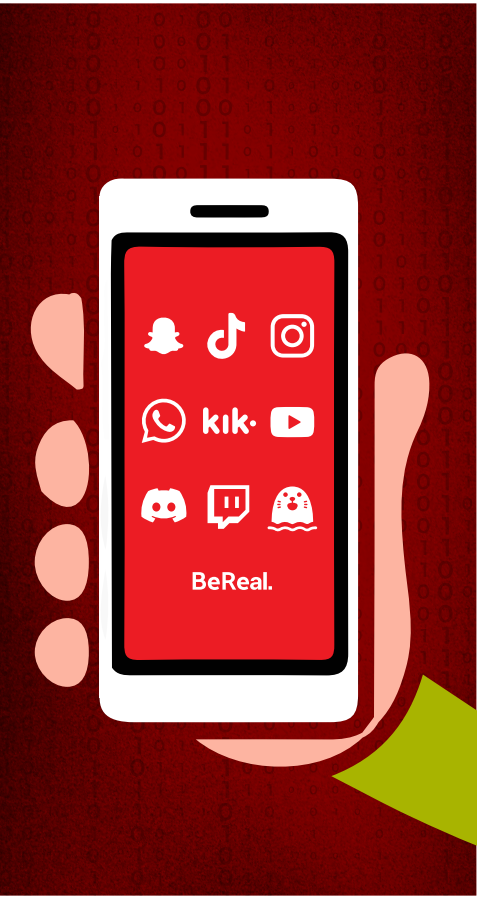
UPDATE YOUR CHILD'S SCHOOL

For serious incidents, update your child's school and any significant adults in their lives (e.g. sports coaches or youth leaders) so that they can monitor and look out for your child.

ESTABLISH A SAFETY AGREEMENT

Teach your child about what will help them stay safe online. Ask them how they are feeling and how they keep safe online. If you don't already have them in place, explore parental controls for your child's device(s).

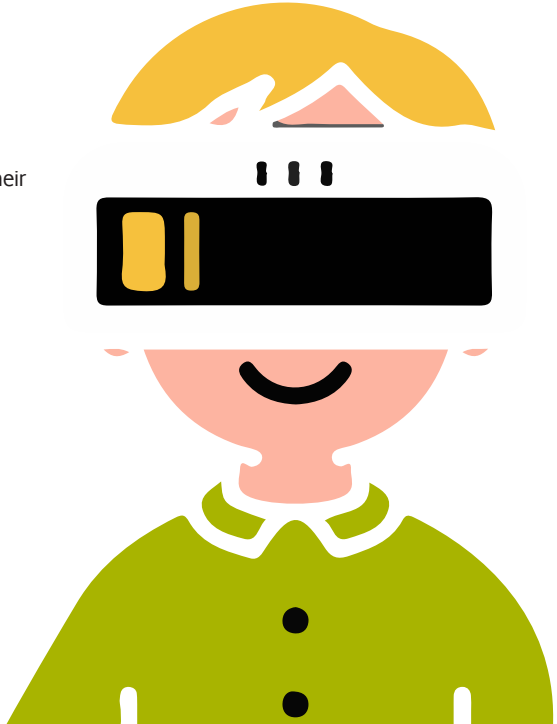
Resources and further reading on cyberbullying and wider issues such as online privacy, or understanding the risk of online scams and grooming can be found on **www.ispcc.ie**, **www.childline.ie**, **www.cybersafekids.ie** and **www.unicef.org**.



Guide to Social Media Apps

The following are some of the most popular social media platforms, along with some of the risks and ways you can help to reduce them. As with all areas of your child's online world, it's important to talk openly with your child about how to enjoy them safely.

For detailed information on how to implement parental controls on each platform, please see their respective websites.



TikTok

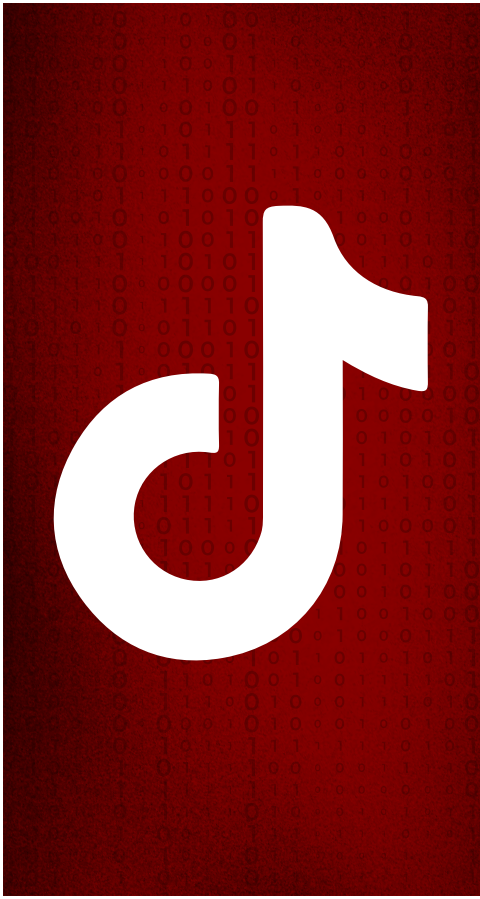
TikTok is a video-sharing app that lets users view and create content using filters, sound effects and background music. Users must be at least 13 years old to have an account on the platform.

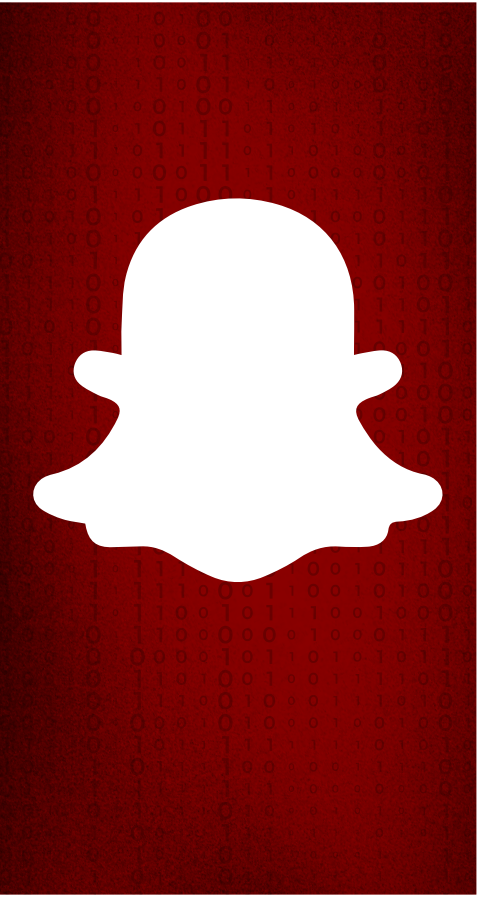
Some of the risks include:

- Exposure to inappropriate content
- Children can easily connect with strangers through comments, direct messages and 'duets'
- Privacy concerns regarding collection of personal data

What you can do:

Family Pairing allows parents to link their TikTok account to their child's and set parental controls including restricting screen time, direct messaging, comments and ensuring your child's account is on private.





Snapchat

Snapchat allows users to send picture, video and text messages that self-destruct after a few seconds. Users must be at least 13 years old.

Some of the risks include:

- False sense of security with disappearing messages, screenshots can still be taken
- Exposure to explicit content through public stories and 'Discover' section
- Potential risk for cyberbullying
- Snap Maps feature which shares the user's location

What you can do:

Use privacy settings to limit who can contact your child, and turn off live location sharing. Talk to your child about the risks of the platform - even though images disappear, they can be screenshotted and then shared.

Instagram

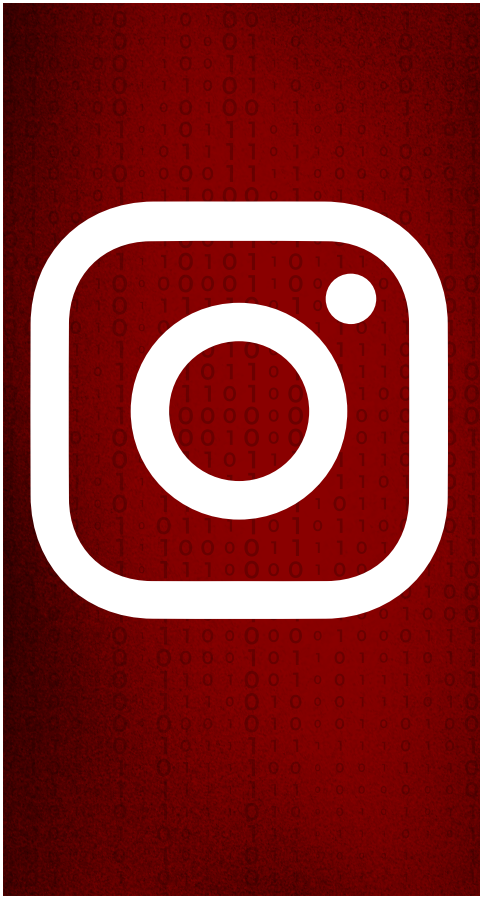
Instagram is a photo and video sharing app where users upload photos or videos to share them with their followers or with a select group of friends. They can also view, comment and like posts shared by others. Users must be at least 13 years old.

Some of the risks include:

- Easy to connect with strangers through comments, direct messages and public posts
- Pressure to maintain a certain image through curated posts and filters
- Negative comparison to others which can affect their mental health

What you can do:

Ensure their account is kept on private mode. Track and limit the amount of time they spend on the app through 'Screen Time' in their phone settings.



WhatsApp

WhatsApp is a messaging app that lets users share messages, images and voice notes directly or through larger group chats. Users must be at least 13 years old.

Some of the risks include:

- Potential for contact with strangers through group chats and forwarded messages
- Privacy concerns regarding the sharing of personal info and metadata
- Can be a channel for cyberbullying

What you can do:

Educate yourself and your kids about the privacy settings, risks and safe usage of the platform.

Kik

Kik is a messaging app that prioritises anonymity. It has a Google age rating of 17+, and the app itself says that teens between the ages of 13 and 18 require parental consent.

Some of the risks include:

- Anonymity is central to the app – it allows for contact with strangers without verification of identity
- Anyone using Kik can send messages to other users without their permission. This could be dangerous as criminals may communicate with teens anonymously
- Exposure to explicit content through public groups and direct messages
- Potential for grooming by predators due to lack of parental controls

What you can do:

Due to lack of parental controls and oversight, much of the advice suggests that this platform is best avoided for a younger audience. Install a third-party parental control app to avoid installation of the app. Or if your child is using Kik, have an open discussion about the risks of the platform.

YouTube

YouTube is a video sharing platform where users can watch, like, share, comment and upload their own videos. Must be 13 to have your own account but children of all ages may use if enabled by a parent or guardian.

Some of the risks include:

- Exposure to explicit content such as violence, explicit language, adult only content, disturbing imagery/videos
- Can become addictive – risk of excessive screen time

What you can do:

YouTube allows parental oversight when you set up Restricted Mode, Supervised Accounts or YouTube Kids accounts as well as providing Safe Search options.

BeReal

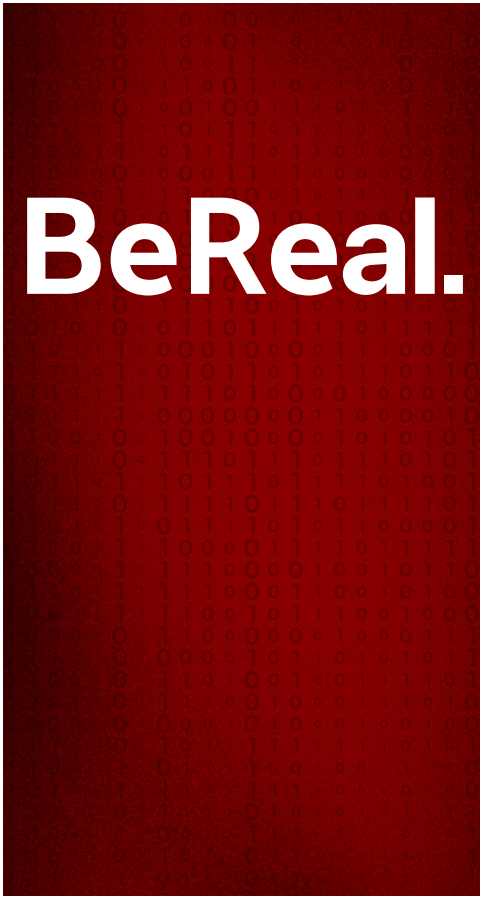
BeReal is a social media app that asks users to post unfiltered photos of themselves once a day. The app sends out a notification at random times prompting users who then have two minutes to take a photo and post it. Users must be 13 years of age or older.

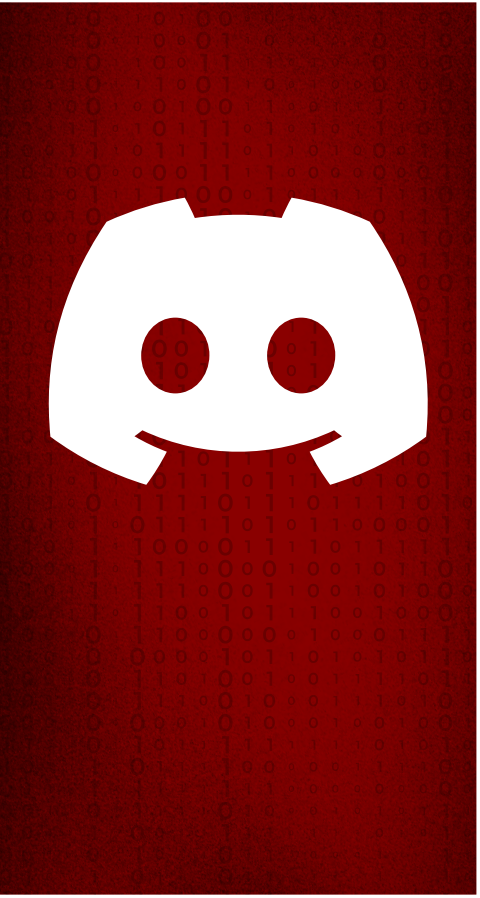
Some of the risks include:

- Strangers can find your kids. The Discovery page is filled with random people who choose to share a photo with the public
- BeReal shares your location by default

What you can do:

Turn off location permission so that posts are not automatically tagged with the location. BeReal does not have any specific parental control features so it's important to remind kids to avoid sharing personal details.





Discord

Discord is a chat app that allows users to chat in real time using text, voice or video. The app hosts servers/chatrooms on different topics and is often used by creators to talk directly to their fans.

Some of the risks include:

- Exposure to explicit content and discussion in public servers
- Interaction with strangers through voice chat and direct messaging
- Potential for cyberbullying/harassment within servers

What you can do:

Discord offers limited parental controls in the form of Family Center, an opt-in tool parents can use to keep tabs on the Discord activity of their children. Family Center provides parents with an activity dashboard they can access through their Discord account, along with an email summary of activity sent out each week.

Twitch

Twitch is a video live-streaming service that focuses on video game live streaming and sports broadcasts. Twitch is not suitable for users under 13 and must have parental permission for users under 18.

Some of the risks include:

- Exposure to inappropriate content
- Potential for cyberbullying/harassment
- Interaction with strangers

What you can do:

Enable chat filter to block hostile or profane language. Make use of report and block features. Change the moderation settings to block harmful content.

HOLLA

HOLLA is a live video-streaming app that randomly matches people in video chats across the globe. Users swipe left or right on other users' profiles to accept or decline live chats with them. It is intended for use by those over the age of 18.

Some of the risks include:

- Encounter with strangers through random video chats, which could include inappropriate content
- There is a lack of control over who users connect with – you have no idea who your child is speaking to

What to do:

HOLLA limits usage to those over 18. Use a parental control tool to block access to HOLLA, so your child isn't able to use the app. Discuss the dangers behind random video chat apps like HOLLA so your child understands why you're restricting their access to it.

Together we can