

PARENT AND CAREGIVER

ONLINE SAFETY GUIDE

Developed by Day One RI
September 2021



TABLE OF CONTENTS

2

INTRODUCTION

4

ABCS OF ONLINE SAFETY

10

APP AWARENESS

22

THE "TALK"

24

THE LAWS

32

RESOURCES



INTRODUCTION

The internet has allowed us the freedom to connect with virtually anyone from the comfort of our homes on screens that are small enough to fit in our pockets and be carried with us throughout the day. We have never had more opportunity for connection, even during times of social distancing. Unfortunately, with so much opportunity to connect, comes vulnerability and risk for exploitation. With so much of our lives happening online, it is no surprise to advocates and prevention practitioners that sexual violence has permeated the digital landscape. Harassment and exploitation are serious issues that should never be tolerated, whether they happen in person or online.

ACKNOWLEDGEMENTS

We would like to thank our partners from the Rhode Island Department of Health who have funded the development of much of the information contained in this guide through their Rape Prevention Education and Prevention Block Grant - Sexual Violence Prevention Program. The production of this guide was also funded by the New England Coalition Against Trafficking (NECAT).

NECAT received \$211,135 through competitive funding through the U.S. Department of Health and Human Services, Administration for Children and Families, Grant # 90ZV0125. The project will be financed with 100% of Federal funds, and 0% by non-governmental sources. The contents of this material are solely the responsibility of the authors and do not necessarily represent the official views of the U.S. Department of Health and Human Services, Administration for Children and Families



Keeping Your Family Safe Online

Now more than ever young people are spending more time online, and may be vulnerable to being exposed to inappropriate content or exploited by online predators.



Strengthen Safety Measures

- Review browser and search engine privacy and security settings
- Contact your internet service provider (or their website) to enquire about potential parental control options or tools that may be available
- Review privacy settings on social media platforms or apps with your family to make sure you're comfortable with how your data is shared with social media companies and/or advertisers, as well as how visible to the public your accounts may be



Open Communication about Online Activity

- Talk to your family about what apps or sites they (or their friends) use frequently
- Review the risks of sharing personal and family information online
- Discuss the difference between friends we know, but connect with online, and online friends, and how boundaries with these kinds of friends are different
- Set expectations for behavior online that are similar to in-person expectations, such as being respectful, not harassing or bullying others, and not sharing explicit content of themselves or others



Observe with Care

- Set expectations of when and where devices may be used, such as in common areas and not late at night
- Discuss your rules around passwords and your plans to monitor their activity
- Keep an eye out for changes in young people's behavior such as secrecy or agitation around technology, large amounts of unsupervised online time, or withdrawal from family activity
- Be mindful of unexpected calls or gifts, especially if youth attempt to hide these from caregivers, as these may be part of a predator's grooming process



Know the Laws

Federal Laws Prohibit:

- Transfer (or attempt) of obscene matter to minors under 16 years old
- Online enticement or coercion of a minor under 18 to engage in sexual activity
- Online enticement or coercion of a minor to engage in sexual conduct to create a visual depiction

Rhode Island Laws Prohibit:

- Knowingly and intentionally transmitting indecent visual depictions to a person they know or believe to be a minor
- Minors knowingly and voluntarily, without threat or coercion, transmitting an indecent visual depiction of themselves to another person



Report Concerns

- Incidents may be reported to the National Center for Missing and Exploited Children at 1-800-THE-LOST (1-800-843-5878) or www.cybercrime.gov
- Please notify local law enforcement if you or your family are in immediate danger



Resources

- Day One: www.dayoneri.org
- NCMC's NetSmartz: www.missingkids.org/netsmartz/home
- Common Sense Media: commonsensemedia.org
- Culture Reframed: www.culturereframed.org
- Internet Matters: internetmatters.org
- Connect Safety: connectsafety.org

Day One

ABCS OF ONLINE SAFETY

A

APPROPRIATE

Not everything on the internet is appropriate for children. Games and apps will have ratings that can help you decide whether or not specific content is appropriate for your child. Parental controls can also be utilized for all different kinds of devices and services. No single parental control will ensure that children are not exposed to inappropriate content, so it is important to put multiple layers of protection in place and test the effectiveness of these controls.

B

BLOCK

Utilizing controls that allow you to block inappropriate content or inappropriate actors online is a healthy way to establish and reinforce online boundaries. You do not have to endure harassing speech, and choosing to block someone can be an act of self-care.

C

CONSENT

Consent is equally important in the online world, as it is in our physical world. It is important that we obtain consent before sharing content that involves other people or sharing explicit content with others.

D

DISCUSSION

Talking to your children about the internet is your most powerful tool in preventing online exploitation and violence. We know these conversations can be difficult, but no other strategy is more effective than open communication. These resources for parents can be a helpful place to start in framing these conversations.



E

EXPLOITATION

While the internet can provide us with essential connections to resources, information and people, the internet can also leave people, especially young people and the elderly, open to exploitation. The tactics exploiters use typically involve force, fraud, and/or coercion. Exploitative acts online may include, but are not limited to cyberstalking, sextortion, non-consensual sexting, child pornography/child sexual abuse materials, or child sex trafficking.



F

FOLLOWERS

It's important to recognize the difference between friends and followers, even though some social media platforms may use these terms interchangeably. Friends are people with whom we share a caring bond, but followers are people or online entities that are interested in having access to what you post online.



G

GEOLOCATION

Geolocation or location sharing refers to the documentation or sharing of an internet user's physical location based on their online activity. While some apps may only provide or record the general location of the user or proximity to other users, some can be far more specific which has the potential to jeopardize children's physical safety. It is important to know what apps (like Snapchat's "Snap Map") are recording or sharing your locations via their settings.



H

HONESTY

In order for children to be honest with us about their online activity, we must be honest with them about how we intend to protect them and what dangers they may encounter online. Have conversations early, and you can begin to build an honest, trusting relationship about internet safety.



IMAGES

In 2020 there were over 50 billion images on Instagram. It is important to think about the digital footprint you are leaving behind when deciding to post something online. Once an image is uploaded to the internet, it can be nearly impossible to get it removed.



JUDGEMENT

It is important to use good judgement while online. If something feels off, take a moment to listen to your gut and think through the consequences of your online behavior. We can create a better, safer online world if we use our best judgement and refrain from judging others.



KIDDLE

Kiddle is a child-friendly search engine that helps youth find factual information to enhance their learning while filtering out inappropriate content. No filtering technology is perfect, so it is important to use multiple parental control strategies to limit exposure to inappropriate content.



LAWS

There are federal and state laws that prohibit multiple forms of online exploitation. Federal law prohibits the transfer of obscene materials to minors under 16 years old and the online enticement of minors to engage in sexual activity or to create a visual depiction of sexual activity. Rhode Island state law prohibits the transfer of indecent visual depictions to a minor, as well as minors transmitting an indecent visual depiction of themselves without force or coercion.

M

MONITORING

While this shouldn't be the first step you take in promoting online safety in your home, for young children or children who have a pattern of violating online trust, monitoring online activity is an option. This may mean turning in phones at a certain time or using programs that allow remote viewing of online activity. It is important that youth know that their activity is being monitored in order to promote trust and open communication about online activity.

N

NETSMARTZ

The National Center for Missing and Exploited Children (NCMEC) has a wonderful program called NetSmartz that teaches online safety concepts to children and teens, as well as providing resources for caregivers and educators. NetSmartz is designed as a curriculum, but these tools can also be used to spark conversation and learning about online safety at home.

O

OBSERVE

It is important to be aware and observe how children are interacting with the internet. Observing is different than monitoring, and may be a less intrusive option, especially for older children. This may mean keeping technology in common spaces and being aware of how much time children spend online.

P

PRIVACY

Engaging with the internet means agreeing to giving up some sort of privacy. Ever wonder why that thing you just Googled is now being advertised on your Facebook? Even simple things like internet browsing data are captured. Every application has their own privacy settings, and it is important to be aware of what you are in control of.



QUIET

According to Common Sense Media, teenagers spend an average of nine hours per day online. Incorporating some “quiet time” into your schedule where you spend time away from the internet or technology is essential for creating balanced, healthy lives.



REPORT

If you encounter illegal or exploitative behavior or content online, it is important to report it to the proper authorities to prevent further harm. Individual apps also have methods to report things like hate speech, harassment, or other forms of abusive content.



SAFETY

Safety should always be the first priority when considering online behavior. Here are five helpful tips on how to prioritize safety while kids spend more time online at home.



TEXTING

Texting is the most used feature on cell phones and has become one of the most common forms of communication. While this method of communication may seem to have replaced casual conversation in many ways, it is important to consider the implications of how these conversations are recorded and can be easily shared with others.



UPLOAD

Everytime we upload something to the internet, we lose control of where that information goes and who has access to it. Make sure to review the privacy settings before posting something online, but always take a moment to consider whether or not you would be comfortable with anyone being able to see what you are uploading.



V

VIDEO GAMES

While video games can be a fun, engaging past-time, almost all online games now have a social component that you might not be aware of! Most mobile games allow you to chat with other players or connect your game to social media accounts. There are also video-game streaming services, like Discord, that may leave children vulnerable to online-grooming.



W

WEBCAM

Webcams allow us more virtual face to face contact, which have proven invaluable in the time of social distancing. It is important to be mindful of your surroundings when using a webcam and to be aware of when your device's webcam is enabled. A prudent option that may work for some is to place tape or a post-it over their webcams when not in use.



X

X-RATED

Inappropriate, x-rated content has never been more available to young viewers than it is in our digital age. When a child reports being exposed to online pornography, it is equally important to discuss their feeling about what they saw, as it is about how they came across it.



Y

YOUTUBE

YouTube is the most popular video-sharing website and application. While there is an endless amount of child-friendly, informative content available on this site, it is important to pay attention to parental controls. Users have reported that the site's algorithms for autoplaying continuous videos have led to young viewers being exposed to inappropriate content.



Z

ZOOM-BOMBING

Zoom has become instrumental for distance learning and remote work for many during the pandemic. Unfortunately, seemingly private conversations can be invaded or inappropriate content can be shared if security settings are not properly managed for these virtual meeting spaces.

APP AWARENESS

In our ever-changing technological landscape, internet safety is a vital priority in ensuring the healthy lives of children. It is important to know what children are doing online, what technologies exist that can potentially leave them vulnerable to exploitation and to have honest conversations about online safety. There are a few distinct elements in online applications that are concerning to maintaining online child safety.



LIVESTREAMING/VIDEO CHAT

Many apps center around providing a platform where users can broadcast their lives live to online viewers. Broadcasters can feel pressured to do things that make them feel uncomfortable in response to viewers' comments and with the goal of putting on an entertaining "performance."



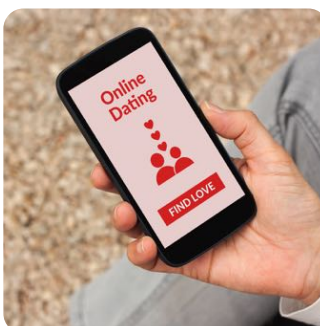
OPEN FORUM/LARGE GROUPS

Many apps create an open forum where users are able to interact globally with any other user of the app. While some make private profiles available, they are not the default setting. Others allow for interaction between members of large groups, all of which children may not be familiar with.



LOCATION SHARING

Many apps access your location via GPS. While some apps may only provide information about your general vicinity to other users, some apps can be far more specific. Many apps also encourage users to seek out contact with other users in their area which could jeopardize children's physical safety.



DATING CONNOTATIONS

Some apps make it clear that their purpose is to facilitate dating relationships through their name, icon or description. However, some may be more vague in their presentation. Some may also describe themselves as an app to find new friendships, but use of the app often reflects a dating motive.



GIFT GIVING SYSTEMS

Some apps have created systems within their platforms which allows users to exchange gifts. This can be something as trivial as a special emoji, but some apps have gifting systems that are redeemable for actual cash. Gift giving is a known grooming strategy for those targeting children, making these systems especially concerning.



RANDOM CONNECTIONS

Some apps facilitate random connections between users. These are often unpredictable, although some provide information to users before making the connection. These connections make children vulnerable by exposing them to unknown users who may take advantage of the surprising nature of the encounter.



TEMPORARY MESSAGES

Some apps have created messaging systems where messages self-destruct after a set period of time. Thinking that there is no permanent record of their online activity, children may behave more impulsively online. Unfortunately, there are still ways for their online activity to be recorded by other users which leaves them vulnerable to exploitation. These systems also prevent parents from being able to accurately monitor their child's online activity.



REPORTS OF GROOMING

Reviews of these apps indicate user experiences that reflect attempts by others to groom young users into an exploitative relationship or who otherwise made inappropriate requests of users. This may involve the request of pictures, more private chats, keeping their interactions a secret, or asking the user to engage with them on another, more private app.





FACEBOOK

Purpose/Use

Facebook is a social networking app made for sharing photos and video. Your Timeline or “newsfeed” is made up of content from friends, advertisements, groups, and “suggested” material.

Major Concerns

- Direct Messaging
- Location Sharing
- Marketplace & Dating Interface
- Cyberbullying

Parent & Privacy Controls

How to set your profile to Private:

1. Select the arrow in the upper-right hand corner of any Facebook screen.
2. Select **Settings & Privacy** in the drop-down menu then choose **Settings**.
3. Select **Privacy** in the left pane.
4. The first item listed is **Who can see your future posts**. If it says **Public**, select **Edit** and choose **Friends** from the drop-down menu.
5. Select **Close** to save the change.

Access Facebook's Protecting Privacy and Security Guidebook:

<https://about.facebook.com/actions/protecting-privacy-and-security/>

How to Report/Block:

To report a post:

1. Go to the post you want to report.
2. Click the **...** in the top right of the post.
3. Click **Find support or report post**.
4. To give feedback, click the option that best describes how the post goes against Facebook's Community Standards. Click **Next**.
5. Depending on your feedback, you may then be able to submit a report to Facebook. For some types of content, Facebook doesn't ask you to submit a report, but Facebook uses your feedback to help their systems learn. Click **Done**.


To block a user:

1. Click on the arrow on the upper-right corner of your Facebook page
2. Select **Settings & Privacy** in the drop-down menu then choose **Settings**.
3. Select **Blocking** in the left pane.
4. Select **Block users** section in the center of the page, and type the person's name or part of their name into the field.
5. A list will come up of names that fit what you typed in. Find the person you want to block and click the **Block** button next to their name.



FACEBOOK (CONT.)

How to Have Sexually Explicit Content Removed

1. Find the image or video you want to report in the app
2. Tap  in the righthand corner of the image.
3. Tap **Find Support or Report Photo**.
4. Select **Something Else**.
5. Select **Non-consensual Intimate Images** and tap **Next**.
6. Check the box that says, "**I believe this goes against Facebook's Community Standards**" and tap **Report**.

Messaging

Facebook has integrated a direct messaging system through their companion app, "Facebook Messenger". You can send anyone a message on Facebook, but if you are not already friends these messages will be sent as a message request first. You can also set privacy settings in Messenger to disallow message requests, so you will never see messages from people who are not Facebook friends.

Terminology

Follow: Follow is a way to keep up with people or entities you're interested in, even if you're not friends. The Follow button is always a way to fine-tune your News Feed to get the types of updates you want to see.

Groups: Facebook Groups allows you to connect with specific sets of people, such as coworkers or family. They're dedicated spaces where you can share updates, photos, and documents as well as message other Group members.

Like: Clicking Like is a way to give positive feedback and connect with things you care about. When you Like something, it appears as an update on your Timeline. Liking a post means you were interested or enjoyed a post, without leaving a comment. Liking a Page means you're connecting to that Page, so you'll start to see its stories in your News Feed. This will be included on your profile, and your name will be listed on the Page as a someone who has Liked it.

News Feed: Your News Feed is a continuously updating list of posts on your homepage. It includes status updates, photos, videos, links, etc. from the people, Pages, and Groups your profile is associated with.

Timeline: Your Timeline is a part of your profile where you can see your posts or posts you've been tagged in displayed by date.

Timeline Review: This lets you approve or reject posts that you've been tagged in before they are added to your Timeline. When people you're not friends with tag you in a post, they automatically go to Timeline review.



INSTAGRAM

Purpose/Use




Instagram is a social networking app made for sharing photos and videos from a smartphone. Similar to Facebook or Twitter, everyone who creates an Instagram account has a profile and a news feed. When you post a photo or video on Instagram, it will be displayed on your profile.

Major Concerns

- Live Broadcast
- Tags
- Direct Messaging
- Location Sharing
- Young users
- Pressure on producing content and gaining followers

Parent & Privacy Controls

How to set your profile to Private:

1. Tap  or your profile picture in the bottom right to go to your profile.
2. Tap  in the top right, then tap  **Settings**.
3. Tap **Privacy**.
4. Tap next to **Private Account** to make your account private.

Access Instagram's Teen Safety for Parents Guidebook:

<https://about.instagram.com/community/parents>

How to Report/Block:

To block or unblock someone:

1. Tap their username to go to their profile.
2. Tap (iPhone/computer) or (Android) in the top right.
3. Tap Block/Unblock (iPhone/Android) or Block/Unblock this user (computer).
4. Tap Block/Unblock again to confirm.

People aren't notified when you block them and their likes and comments will be removed from your photos and videos. Unblocking someone won't restore their previous likes and comments.





INSTAGRAM (CONT.)

How to Have Sexually Explicit Content Removed

Posting, sharing or downloading images that sexually exploit children for any reason can be criminal. IG reports all apparent child pornography to the National Center for Missing and Exploited Children. If you ever see this type of content on Instagram don't share it or comment on it.

Report it by using the following options:

1. Tap 3 dots on the post ... (iPhone) or (Android) above the post.
2. Tap Report.
3. Follow the on-screen instructions.

Notify the National Center for Missing & Exploited Children using the CyberTipline. If you think an image or video is spreading "virally," please report it instead of sharing or commenting on it.

Messaging

DM means direct messaging. On Instagram, DMs are private messages between one Instagram user and another user or group of users. Instagram DMs don't show up in your brand's feed, profile, or search. Anyone, whether the person follows you or not, can send you direct messages unless this person is blocked.

Terminology

Explore: Explore is where young people will see photos and videos from accounts and hashtags they might be interested in. Explore is different for everyone - the content changes depending on accounts and hashtags your child follows

Feed: Feed is where young people can see posts from the accounts they follow. Young people generally see feed posts as being more celebratory or special. Feed posts can be photos or videos.

IGTV: IGTV is a place to share video content up to one hour in length. Your child can find videos from their favorite creators, and make their own longer content.

Reels: Reels allows people to record and edit short videos up to 30 seconds in the Instagram Camera. You can add effects and music to your reel or use your own original audio.

Stories: Stories disappear from the app after 24 hours, unless your child has enabled archiving, which makes their expired stories available only to them. Your child can subsequently share these in their Stories Highlights. Anyone who can view your child's stories can screenshot them.



TWITTER

Purpose/Use

Twitter is a free microblogging and social networking site with posts limited to 280 characters. On Twitter you can follow accounts from friends, celebrities and organizations. Blue check marks next to usernames indicate that the person that account claims to belong to has been verified. Twitter also monitors and highlights trending topics or stories on its platform.

Major Concerns

- Livestreaming
- Location Sharing
- Influence of users/companies on children
- Easy to find sexually explicit content
- Lack of civility in discourse, including cyberbullying/harassment
- Grooming, as profiles are public by default

Parent & Privacy Controls

How to access controls:

1. Click on profile image to open menu
2. Select **Settings and Privacy**
3. Select **Privacy and Safety**

Protect Your Tweets: Only followers and people you approve can see tweets

Photo Tagging: Only people following you can tag you


Live Video: Leave unticked to disallow live streaming

Discoverability & Contacts: Leave unticked in order to keep people from finding profile via phone number or email address

Safety - Display media that may contain sensitive content: Leave this unticked to keep inappropriate content from showing. Can also manage blocked/muted accounts and muted words under Safety section

How to Report/Block:

To report a harmful or abusive tweet:

1. Click or tap the  icon
2. Select **Report**
3. Select **it's abusive or harmful**
4. You'll be asked to provide more information about the issue, and can select more tweets from the same user as context.
5. Decide if you want to receive updates on the report by selecting **Updates about this report can show this tweet**

For more reporting instructions please visit: <https://help.twitter.com/en/safety-and-security/report-abusive-behavior#video>



TWITTER (CONT.)

To block a profile:

1. Click or tap the  icon on their profile page
2. Select **Block**

For more blocking instructions please visit: <https://help.twitter.com/en/using-twitter/blocking-and-unblocking-accounts#video>

How to Have Sexually Explicit Content Removed

1. Login to your account
2. Click on three dots in top right corner on tweet with content you want removed
3. Tap **It's abusive or harmful**
4. Tap **Includes Private Information**
5. Select **Other**
6. Select the appropriate option based on who you are reporting on the behalf of
7. Additional tweets can be added to the report
8. Tap **Send Report to Twitter**

Can report a profile as well by clicking on three dots on profile page and following same steps

Messaging

Tweets are public messages, while "Direct Messages" or DMs are private. DMs can be found in the bottom right corner of the app with an envelope icon. These messages can be sent/received by anyone, unless you change your account settings.

Terminology

Hashtag (#): These are used to tag key words or trending topics. They encourage discussion and allow the tweet to be viewed by a larger audience. Popular hashtags, topics, and news stories will appear in the 'Explore' section of Twitter.

Mention: Users can mention other people in their tweets by using the '@' sign, followed by the other person's handle. For example, @user123.

Retweet: If somebody 'retweets' a tweet, it means that they've shared it with all their followers.





SNAPCHAT

Purpose/Use

Snapchat is a social networking app that allows users to send time limited messages, images, and videos to other users or as part of stories on user profiles for 24 hours. Snapchat is well known for its filters/lenses and integration of personal avatars called "Bitmojis", but also includes features like "Snap Map" where users can see where friends are in real time.

Major Concerns

- Sending/receiving explicit material
- Grooming, as there is the potential for exposure to strangers, including the ability to send and receive cash
- Location Sharing
- "Discover" page may contain inappropriate content
- Impulsivity may increase due to messages being time-limited

Parent & Privacy Controls

How to access controls:

1. Tap profile avatar in top right corner
2. Tap  to open **Settings**
3. Scroll to **Who can... (Contact Me, View My Story, See My Location, See Me in Quick Add)**

There are no child safety settings for the "Discover" page, though stories can be individually "hidden".

The content is generated using an algorithm based on search and view history.

To access Snapchat's parent guide please visit:

<https://support.snapchat.com/en-US/article/parent-guide>

How to Report/Block:

To block or report a user:

1. Tap the user profile image
2. Tap three dots in right top corner
3. Tap **Report** or **Block**

How to Have Sexually Explicit Content Removed

To make a complaint about a story or snap:

1. Press and hold the Snap until a flag icon appears in the bottom left corner
2. Tap on the flag to begin a report
3. Select the appropriate reporting option (a comment box is provided for more detailed information)
4. Submit the report
5. Decide if you want to block the user

If you don't have an account or are unable to report a safety concern in-app, you can report issue on the [Snapchat Support site](https://support.snapchat.com/en-US/article/parent-guide).

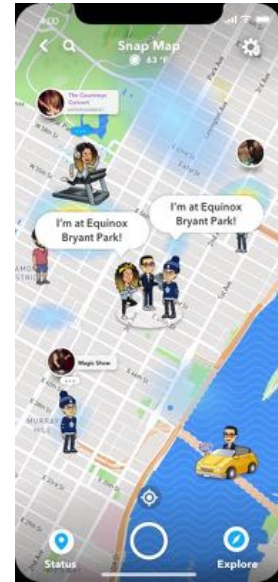


Image: SnapMap Source: Snapchat Support



SNAPCHAT (CONT.)

Messaging

Depending on the message security settings, users can message others and these disappear after 24 hours unless saved by a user within the conversation. Even picture messages which are deleted within a specific time frame of opening the message, can be saved by the recipient by screenshotting the open message. While Snapchat alerts a sender if a message was screenshot, there is no way for the sender to keep the recipient from saving the screenshot, and some users have found tricks to keep those alerts from being sent in the first place.

Terminology

Discover: Discover is a section created for brands and publishers to develop Snapchat Stories for the app's large audiences. On Discover, users can find branded content made by Vice, Cosmopolitan, Daily Mail, ESPN, Tastemade, CNN, BuzzFeed, and more. To access Discover, click on a branded icon, slide through the contents, and swipe up to see more information about a particular Snap, Story, or brand.

Filters: Filters are additions that users can select to decorate their Snaps. To add a filter, simply snap a photo or a video then swipe left to see what filters are available.

Friend Emojis: Snapchat's friend emojis signify how frequently one sends a Snap to another user. An emoji that looks like an hourglass, for example, means that a user's "Snapstreak" (i.e. how often they communicate with that particular user via Snapchat) is about to end, and a birthday cake emoji appears when it's a user's birthday. For a comprehensive list of what each friend emoji means, go to Settings → Manage → Friend Emojis.

Lenses: One of the most innovative and popular features on Snapchat, lenses integrate with a user's face to create entertaining animations and overlays that enhance a user's Snaps. To activate the lenses, press and hold on the face in a snap and follow the directions (such as "open mouth"). Different lenses are released each day, and many brands have reached millions by developing custom branded lenses.

On-Demand Geofilters: Like filters, Geofilters decorate a user's Snaps. Unlike regular filters, however, Geofilters are specific to a user's location or an event they are attending and can be used to generate engagement and encourage Snapchat users to share their experiences with friends and followers. On-Demand Geofilters may even be designed and purchased by individuals or smaller companies and only become available when a Snapchat user enters a specified geo-location.

Snapcash: The result of a partnership between Snapchat and Square, Snapcash allows Snapchat users to transfer money to their friends. To access Snapcash, users must enter their debit card information, then text "\$ + the amount they want to send" (e.g. "\$5" for 5 dollars) to another Snapchat user.

Snap Map: On Snap Map, users can view Snaps submitted to Snap Map from all across the world — including sporting events, celebrations, breaking news, and more. Users and their friends can also share their locations with each other and see what's going on around you.



TIKTOK

Purpose/Use

TikTok is a social networking app that lets you watch, create, and share videos, often with music or as part of dance “challenges”

Major Concerns

- Live Broadcast
- Virtual Gift Giving
- Inappropriate Content
- Pressure on producing content and gaining followers

Parent & Privacy Controls

On TikTok, parents can set time limits, filter mature content and disable direct messaging for children's accounts. You can enable time limits and the content filter on child's phone and protect the settings with a passcode, but to disable direct messaging you need to use the app's Family Pairing feature, which also gives you access to time limits and content filters). Keep in mind that children can always redownload an app and create a new account using a different phone number or email address, so these controls are not foolproof and should be viewed as only one layer of protection.

Screen Time Management: This setting limits users to a maximum of two hours on the app per day, but you can limit it to 40 minutes. If you're only enabling this on your child's phone, choose a passcode to lock the setting.

Restricted Mode: This blocks mature content, but even with the filter on, children using the app on their own might come across age-inappropriate content. This setting can also be locked with a passcode.

Family Pairing: To set up Family Pairing so you can manage settings and disable direct messaging, first download TikTok onto your phone and create an account. Then, make sure you have your child's phone and their login handy. On both phones tap the three dots next to their user profile. Tap **Family Pairing** and sync your account to their phone via the QR code.

How to Report/Block:

To block or report someone:

1. Go to the user profile.
2. Click the three dots on the bottom right corner.
3. Click **Report/Block**.

How to Have Sexually Explicit Content Removed

Follow the same instructions above to report and select the most appropriate response as the reason for the report, like **Posting Inappropriate Content** or **Nudity or Pornography**.



TIKTOK (CONT.)

Messaging

Like many other social media apps, TikTok has direct messaging as a feature. TikTok has added restrictions that only allow users over the age of 16 to use this feature. Users can also only message other users that they are following and if messaging is enabled in the privacy settings. You can also change who (everyone, friends, or no one) is allowed to send you direct messages in your privacy settings.

Terminology

Challenges: TikTok challenges are viral trends that users incorporate into the videos usually involving a specific task or dance. Challenges can have dangerous or inappropriate themes. For example, challenges in the past have included users choking themselves on video until they blackout or taking enough Benadryl to induce hallucination. The #SilhouetteChallenge encouraged users to show off their bodily figures by masking nudity with a red filter. Some users found ways to remove this filter from already posted videos, exposing users bodies without their consent.

Duet: Duet videos allow users to take another user's video and add their own video alongside it.

Fans: If you are enthusiastic about the content of another user, you can become a 'fan' and follow their profile to make sure you don't miss any of their activity.

Hearts: You can show your admiration for a video by clicking the heart on the right-hand side of the screen. Clicking the heart will auto-generate a collection within your own profile, collecting all of your favorite videos so you can view them later.



THE "TALK"

We are living in an ever-growing, digitally connected world. Online spaces often leave youth vulnerable to exploitation and harmful information. Parents should discuss online safety and limitations regularly.

AGES 2-6

Supervision

At this age children do not have the critical thinking skills necessary to be safe online unsupervised and screen time should be extremely limited.

Setting Limits

As children get a little older they may be slowly introduced to using the internet with significant limitations. Figure out what they want and are allowed to do online, and set bookmarks for specific websites.

You can watch one video on my phone, but I have to watch it with you.

You can use the internet to go to specific websites or play specific games with my permission, but we need to make sure we stay on the same website and be careful about what we click on.

I want us to start building trust about using the internet. You can't use these devices behind closed doors, and there will be limits on what you can do.

We can't be sure people are who they say they are online, so we shouldn't tell people our full names or information about where we live.

I want you to learn how to use the internet safely, but you're not ready to talk to other people online yet. When you get a little older we'll talk about how you can safely connect with approved friends or family members.

AGES 7-12

Developing Independence Online

Younger children in this age group should still be supervised while online, but older children should be building to independence. Keep internet enabled devices in common living areas and utilize parental controls to compliment supervision.

Personal Information

Children at this age are vulnerable to scams and marketers mining personal data. Teach them to come to you before sharing any personal information online and explain why and when it is unsafe to do so.

Online Activities

Talk to children about their online activities as you would any offline activities. Get to know what they like to do and who they might be doing it with. Discuss limitations like disallowing chat rooms, messaging or social media.

AGES 13+

House Rules:

Establish ground rules for all internet use that works for your family. Have them share login information with you and do periodic check-ups on their browsing history or account use. Being open about this can build trust.

Responsible Online Behavior

While youth are gaining independence online, they may test the limits to determine where their boundaries are. Make sure to be clear about what your expectations are and what you consider to be responsible online behavior.

Online Friends

Youth will likely begin connecting with friends online that they know in real life. However, as they begin to use social media and multi-player online games, they may begin to form relationships with people they have never met before. It is important to help them make the distinction and understand the differences in boundaries between the two. Help them recognize the signs of online grooming from those who would do harm.

I need to know that you're able to use these accounts and sites responsibly. I'm going to be checking in on how you're using them, and if I see something worrying, we'll talk about it.

We do not use the internet to gossip, bully, or threaten anyone. If we wouldn't say it in person, we shouldn't be saying it online.

It's nice to stay in touch with our friends and family online, but there are also people out there who we don't know, and some of them are dangerous. If you get a request or message from someone and you're not sure who they are, come talk to me first.

Remember, we never share personal information or agree to meet in person with anyone we met online.



THE LAWS

This section outlines Federal and Rhode Island General Laws that apply to online activities and online safety. Some of these laws are specific to minors, but most apply to adults as well. These laws are provided as a summary and do not represent an exhaustive list.

FEDERAL LAWS

18 USC 1466A: Obscene visual representations of the sexual abuse of children

(a) In General.-Any person who, in a circumstance described in subsection (d), knowingly produces, distributes, receives, or possesses with intent to distribute, a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting, that-

(1)(A) depicts a minor engaging in sexually explicit conduct; and

(B) is obscene; or

(2)(A) depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; and

(B) lacks serious literary, artistic, political, or scientific value; or attempts or conspires to do so, shall be subject to the penalties provided in section 2252A(b)(1), including the penalties provided for cases involving a prior conviction.

18 USC 1470: Transfer of obscene material to minors

Whoever, using the mail or any facility or means of interstate or foreign commerce, knowingly transfers obscene matter to another individual who has not attained the age of 16 years, knowing that such other individual has not attained the age of 16 years, or attempts to do so, shall be fined under this title, imprisoned not more than 10 years, or both.

18 USC 2251: Sexual exploitation of children

(a) Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

(b) Any parent, legal guardian, or person having custody or control of a minor who knowingly permits such minor to engage in, or to assist any other person to engage in, sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct shall be punished as provided under subsection (e) of this section, if such parent, legal guardian, or person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

(c)(1) Any person who, in a circumstance described in paragraph (2), employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, any sexually explicit conduct outside of the United States, its territories or possessions, for the purpose of producing any visual depiction of such conduct, shall be punished as provided under subsection (e).

(2) The circumstance referred to in paragraph (1) is that-

(A) the person intends such visual depiction to be transported to the United States, its territories or possessions, by any means, including by using any means or facility of interstate or foreign commerce or mail; or

(B) the person transports such visual depiction to the United States, its territories or possessions, by any means, including by using any means or facility of interstate or foreign commerce or mail.

(d)(1) Any person who, in a circumstance described in paragraph (2), knowingly makes, prints, or publishes, or causes to be made, printed, or published, any notice or advertisement seeking or offering-

(A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or

(B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

shall be punished as provided under subsection (e).

(2) The circumstance referred to in paragraph (1) is that-

(A) such person knows or has reason to know that such notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed; or

(B) such notice or advertisement is transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed.

(e) Any individual who violates, or attempts or conspires to violate, this section shall be fined under this title and imprisoned not less than 15 years nor more than 30 years, but if such person has one prior conviction under this chapter, section 1591, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, abusive sexual contact involving a minor or ward, or sex trafficking of children, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 25 years nor more than 50 years, but if such person has 2 or more prior convictions under this chapter, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to the sexual exploitation of children, such person shall be fined under this title and imprisoned not less than 35 years nor more than life. Any organization that violates, or attempts or conspires to violate, this section shall be fined under this title. Whoever, in the course of an offense under this section, engages in conduct that results in the death of a person, shall be punished by death or imprisoned for not less than 30 years or for life.

18 USC 2260: Production of sexually explicit depictions of a minor for importation into the United States

(a) Use of Minor.-A person who, outside the United States, employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor with the intent that the minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, intending that the visual depiction will be imported or transmitted into the United States or into waters within 12 miles of the coast of the United States, shall be punished as provided in subsection (c).

(c)(1) Any person who, in a circumstance described in paragraph (2), employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, any sexually explicit conduct outside of the United States, its territories or possessions, for the purpose of producing any visual depiction of such conduct, shall be punished as provided under subsection (e).

(2) The circumstance referred to in paragraph (1) is that-

(A) the person intends such visual depiction to be transported to the United States, its territories or possessions, by any means, including by using any means or facility of interstate or foreign commerce or mail; or

(B) the person transports such visual depiction to the United States, its territories or possessions, by any means, including by using any means or facility of interstate or foreign commerce or mail.

(d)(1) Any person who, in a circumstance described in paragraph (2), knowingly makes, prints, or publishes, or causes to be made, printed, or published, any notice or advertisement seeking or offering-

(A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or

(B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

shall be punished as provided under subsection (e).

(2) The circumstance referred to in paragraph (1) is that-

(A) such person knows or has reason to know that such notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed; or

(B) such notice or advertisement is transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed.

(e) Any individual who violates, or attempts or conspires to violate, this section shall be fined under this title and imprisoned not less than 15 years nor more than 30 years, but if such person has one prior conviction under this chapter, section 1591, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, abusive sexual contact involving a minor or ward, or sex trafficking of children, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 25 years nor more than 50 years, but if such person has 2 or more prior convictions under this chapter, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to the sexual exploitation of children, such person shall be fined under this title and imprisoned not less than 35 years nor more than life. Any organization that violates, or attempts or conspires to violate, this section shall be fined under this title. Whoever, in the course of an offense under this section, engages in conduct that results in the death of a person, shall be punished by death or imprisoned for not less than 30 years or for life.

18 USC 2261A: Stalking

Whoever-

(1) travels in interstate or foreign commerce or is present within the special maritime and territorial jurisdiction of the United States, or enters or leaves Indian country, with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, and in the course of, or as a result of, such travel or presence engages in conduct that-

(A) places that person in reasonable fear of the death of, or serious bodily injury to-

(i) that person;

(ii) an immediate family member (as defined in section 115) of that person;

(iii) a spouse or intimate partner of that person; or

(iv) the pet, service animal, emotional support animal, or horse of that person; or

(B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of subparagraph (A); or

(2) with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that-

(A) places that person in reasonable fear of the death of or serious bodily injury to a person, a pet, a service animal, an emotional support animal, or a horse described in clause (i), (ii), (iii), or (iv) of paragraph (1)(A); or

(B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A), shall be punished as provided in section 2261(b) or section 2261B, as the case may be.

18 USC 2261B: Enhanced penalty for stalkers of children

(a) In General.-Except as provided in subsection (b), if the victim of an offense under section 2261A is under the age of 18 years, the maximum imprisonment for the offense is 5 years greater than the maximum term of imprisonment otherwise provided for that offense in section 2261.

(b) Limitation.-Subsection (a) shall not apply to a person who violates section 2261A if-

(1) the person is subject to a sentence under section 2261(b)(5); and

(2)(A) the person is under the age of 18 at the time the offense occurred; or

(B) the victim of the offense is not less than 15 nor more than 17 years of age and not more than 3 years younger than the person who committed the offense at the time the offense occurred.

18 USC 2422: Coercion and enticement (a) Use of Minor

(a) Whoever knowingly persuades, induces, entices, or coerces any individual to travel in interstate or foreign commerce, or in any Territory or Possession of the United States, to engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title or imprisoned not more than 20 years, or both.

(b) Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life.

RHODE ISLAND GENERAL LAWS

§ 11-9-1.3. Child pornography prohibited.

((a) Violations. It is a violation of this section for any person to:

- (1) Knowingly produce any child pornography;
- (2) Knowingly mail, transport, deliver or transfer by any means, including by computer, any child pornography;
- (3) Knowingly reproduce any child pornography by any means, including the computer; or
- (4) Knowingly possess any book, magazine, periodical, film, videotape, computer disk, computer file or any other material that contains an image of child pornography.

(b) Penalties.

(1) Whoever violates or attempts or conspires to violate subdivisions (a)(1), (a)(2) or (a)(3) of this section shall be subject to a fine of not more than five thousand dollars (\$5,000), or imprisoned for not more than fifteen (15) years, or both.

(2) Whoever violates or attempts or conspires to violate subdivision (a)(4) of this section shall be subject to a fine of not more than five thousand dollars (\$5,000), or imprisoned not more than five (5) years, or both.

§ 11-9-1.4. Minor electronically disseminating indecent material to another person - "Sexting" prohibited.

(a) Definitions as used in this section:

- (1) "Minor" means any person not having reached eighteen (18) years of age;
- (2) "Computer" has the meaning given to that term in § 11-52-1;
- (3) "Telecommunication device" means an analog or digital electronic device which processes data, telephony, video, or sound transmission as part of any system involved in the sending and/or receiving at a distance of voice, sound, data, and/or video transmissions;
- (4) "Indecent visual depiction" means any digital image or digital video of the minor engaging in sexually explicit conduct, and includes data stored on any computer, telecommunication device, or other electronic storage media which is capable of conversion into a visual image;
- (5) "Sexually explicit conduct" means actual masturbation or graphic focus on or lascivious exhibition of the nude genitals or pubic area of the minor.

(b) No minor shall knowingly and voluntarily and without threat or coercion use a computer or telecommunication device to transmit an indecent visual depiction of himself or herself to another person.

(c) A violation of this section shall be a status offense and referred to the family court.

(d) Any minor adjudicated under subsection (b) shall not be charged under § 11-9-1.3 and, further, shall not be subject to sex offender registration requirements set forth in § 11-37.1-1 et seq., entitled "Sexual Offender Registration and Community Notification Act."

§ 11-9-1.5. Electronically disseminating indecent material to minors prohibited.

(a) Definitions as used in this section:

- (1) "Minor" means any person not having reached eighteen (18) years of age.
- (2) "Computer" has the meaning given to that term in § 11-52-1.
- (3) "Telecommunication device" means an analog or digital electronic device that processes data, telephone, video, or sound transmission as part of any system involved in the sending and/or receiving at a distance of voice, sound, data, and/or video transmissions.
- (4) "Indecent visual depiction" means any digital image or digital video depicting one or more persons engaging in sexually explicit conduct, is obscene as defined in § 11-31-1(b), and includes:

(i) Data stored on any computer, telecommunication device, or other electronic storage media that is capable of conversion into a visual image; or

(ii) Digital video depicting sexually explicit conduct transmitted live over a computer online service, internet service, or local electronic bulletin board service. If a digital image or digital video is part of a larger work, that larger work shall be the subject for the purpose of § 11-31-1(b) analysis.

(5) "Sexually explicit conduct" means actual:

- (i) Graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, or lascivious sexual intercourse where the genitals or pubic area of any person is exhibited;
- (ii) Bestiality;
- (iii) Masturbation;
- (iv) Sadistic or masochistic abuse; or
- (v) Graphic or lascivious exhibition of the genitals or pubic area of any person.

(b) No person shall knowingly and intentionally use a computer or telecommunication device to transmit an indecent visual depiction to a person he or she knows is, or believes to be, a minor.

(c) No minor shall be charged under this section if his or her conduct falls within § 11-9-1.4, "Minor Electronically Disseminating Indecent Material to Another Person – 'Sexting' Prohibited."

(d) No person shall be charged under this section if the minor to whom the indecent visual depiction was transmitted was fifteen (15) years of age or older and the person transmitting the indecent visual depiction was not more than four (4) years older than the minor.

(e) The fact that an undercover operative or law enforcement officer was involved in the detection and investigation of an offense under this section shall not constitute a defense to a prosecution under this section.

(f) Those in violation of this section shall be guilty of a felony and subject to imprisonment for not more than five (5) years, a fine of not more than five thousand dollars (\$5,000), or both.

(g) Those in violation of this section shall be subject to sex offender registration requirements set forth in § 11-37.1-1 et seq., entitled "Sexual Offender Registration and Community Notification Act."

(h) Nothing in this section shall be construed to impose liability upon the following entities as a result of content or information provided by another person:

- (1) An interactive computer service;
- (2) A provider of public or private mobile service; or
- (3) A telecommunications network provider.

§ 11-37-8.8. Indecent solicitation of a child.

(a) A person is guilty of indecent solicitation of a child if he or she knowingly solicits another person under eighteen (18) years of age or one whom he or she believes is a person under eighteen (18) years of age for the purpose of engaging in an act of prostitution or in any act in violation of chapter 9, 34, or 37 of this title.

(b) As used in this section, the word "solicit" or "solicitation" means to command, authorize, urge, incite, request, or advise another to perform an act by any means including, but not limited to, in person, over the phone, in writing, by computer, through the Internet, or by advertisement of any kind.

Every person who shall commit indecent solicitation of a child shall be imprisoned for not less than five (5) years.

§ 11-52-4.2. Cyberstalking and cyberharassment prohibited.

(a) Whoever transmits any communication by computer or other electronic device to any person or causes any person to be contacted for the sole purpose of harassing that person or his or her family is guilty of a misdemeanor, and shall be punished by a fine of not more than five hundred dollars (\$500), by imprisonment for not more than one year, or both. For the purpose of this section, "harassing" means any knowing and willful course of conduct directed at a specific person which seriously alarms, annoys, or bothers the person, and which serves no legitimate purpose. The course of conduct must be of a kind that would cause a reasonable person to suffer substantial emotional distress, or be in fear of bodily injury. "Course of conduct" means a pattern of conduct composed of a series of acts over a period of time, evidencing a continuity of purpose. Constitutionally protected activity is not included within the meaning of "course of conduct."

(b) A second or subsequent conviction under subsection (a) of this section shall be deemed a felony punishable by imprisonment for not more than two (2) years, by a fine of not more than six thousand dollars (\$6,000), or both.

§ 11-52-7.1. Online impersonation.

(a) Definitions, as used in this section:

(1) "Commercial social networking site" means a business, organization, or other similar entity that operates a website and permits persons to become registered users for the purpose of establishing personal relationships with other users through direct or real-time communication with other users or the creation of web pages or profiles available to the public or to other users.

(2) "Electronic mail" means an electronic mail message sent through the use of an electronic mail program or a message board program.

(3) "Identifying information" means information that alone, or in conjunction with other information, identifies a person, including a person's:

(i) Name, social security number, date of birth, or government-issued identification number;

(ii) Unique biometric data, including the person's fingerprint, voice print, or retina or iris image;

(iii) Unique electronic identification number, electronic mail address, routing code, or financial institution account number; and

(iv) Telecommunication identifying information or access device.

(4) "Public official" means a person elected by the public, or elected or appointed by a governmental body, or an appointed official in the executive, legislative, or judicial branch of the state or any political subdivision thereof.

(b) A person commits the crime of online impersonation if the person:

(1) Uses the name or persona of another person to create a web page on or to post one or more messages on a commercial social networking site or sends an electronic mail, instant message, text message, or similar communication without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person;

(2) Sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, telephone number, or other item of identifying information belonging to any person without obtaining the other person's consent with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication and with the intent to harm or defraud any person; or

(3) Uses the name or persona of a public official to create a web page on, or to post one or more messages on, a commercial social networking site or sends an electronic mail, instant message, text message, or similar communication without obtaining the public official's consent and with the intent to induce another to submit to such pretended official authority, to solicit funds, or otherwise to act in reliance upon that pretense to the other person's detriment.

(c) Every person convicted of an offense under this section shall be guilty of a misdemeanor for the first offense and shall be subject to imprisonment not exceeding one year, a fine of one thousand dollars (\$1,000), or both, and an order of restitution as provided herein. Every person convicted of a second or subsequent offense under this section shall be guilty of a felony and shall be subject to imprisonment not exceeding three (3) years, a fine of three thousand dollars (\$3,000), or both, and an order of restitution as provided herein.

(d) Every person convicted of an offense under this section shall be subject to an order for restitution, if appropriate, which shall be in addition to any other applicable penalty.

§ 11-64-3. Unauthorized dissemination of indecent material.

(a) Definitions as used in this section:

(a) A person is guilty of unauthorized dissemination of a sexually explicit visual image of another person when the person intentionally, by any means, disseminates, publishes, or sells:

(1) A visual image that depicts another identifiable person eighteen (18) years or older engaged in sexually explicit conduct or of the intimate areas of that person;

(2) The visual image was made, captured, recorded, or obtained under circumstances in which a reasonable person would know or understand that the image was to remain private;

(3) The visual image was disseminated, published, or sold without the consent of the depicted person; and

(4) With knowledge or with reckless disregard for the likelihood that the depicted person will suffer harm, or with the intent to harass, intimidate, threaten, or coerce the depicted person.

(b) Subsection (a) shall not apply to:

- (1) A visual image that involves voluntary exposure of intimate areas or of sexually explicit conduct in a public or commercial setting, or in a place where a person does not have a reasonable expectation of privacy;
- (2) Dissemination made in the public interest, scientific activities, or educational activities;
- (3) Dissemination made in the course of a lawful public proceeding;
- (4) Dissemination made for purposes of law enforcement, criminal reporting, corrections, legal proceedings, the reporting of unlawful conduct, or for medical treatment; or
- (5) Dissemination of an image that constitutes a matter of public concern, such as a matter related to a newsworthy event or related to a public figure.

(c) For the purposes of this section, "intimate areas" means the naked genitals, pubic area, buttocks, or any portion of the female breast below the top of the areola of a person that the person intended to protect from public view.

(d) A first violation of this section shall be a misdemeanor and, upon conviction, subject to imprisonment of not more than one year, a fine of not more than one thousand dollars (\$1,000), or both. A second or subsequent violation of this section shall be a felony and, upon conviction, subject to imprisonment for not more than three (3) years, a fine of not more than three thousand dollars (\$3,000), or both.

(e) Any person who intentionally threatens to disclose any visual image described in subsection (a) and makes the threat to obtain a benefit in return for not making the disclosure or in connection with the threatened disclosure, shall be guilty of a felony and, upon conviction, be subject to imprisonment for up to five (5) years, a fine of up to five thousand dollars (\$5,000), or both.

(f) Any person who demands payment of money, property, services, or anything else of value from a person in exchange for removing any visual image described in subsection (a) from public view shall be guilty of a felony and, upon conviction, be subject to imprisonment for up to five (5) years, a fine of up to five thousand dollars (\$5,000), or both.

(g) Those in violation of this section shall not be subject to sex offender registration requirements as set forth in chapter 37.1 of title 11 entitled "Sexual Offender Registration and Community Notification Act."

(h) A violation of this section is committed within this state if any conduct that is an element of the offense, or any harm to the depicted person resulting from the offense, occurs in this state.

(i) Nothing in this section shall be construed to impose liability on an interactive computer service, as defined in 47 U.S.C. § 230(f)(2), an information service, as defined in 47 U.S.C. § 153, or a telecommunications service, as defined in § 44-18-7.1, for content provided by another person.



RESOURCES

The following are national and local resources that provide supportive services, reporting mechanisms, investigation, prosecution and prevention and awareness educational materials.

SERVICES/REPORTING/HEALING

National Center for Missing & Exploited Children (NCMEC) Cyber Tipline: 800-843-5678

Can be used to report instances of child pornography or commercial sexual exploitation of children. Can also be used to communicate information to authorities.
Website: www.missingkids.org

National Child Abuse Hotline: 800-422-2253

The hotline can provide local referrals and connect the caller to a counselor within their call center. They also provide services in over 140 languages.
Website: www.childhelp.org/hotline/

Cyber Civil Rights Initiative Crisis Helpline: 844-878-2274

The CCRI Crisis Helpline provides information, guidance related to image documentation and takedown, referrals to attorneys, and emotional support to victims of non-consensual pornography, recorded sexual assault and sextortion. Victims who reside in the United States can reach the CCRI Crisis Helpline (844-878-CCRI) 24 hours a day, seven days a week. Interpretation is available to callers in most languages.
Website: www.cybercivilrights.org

RI State Police Internet Crimes Against Children Task Force

The Rhode Island Internet Crimes Against Children (ICAC) Task Force is a multi-agency group comprised of sworn federal, state and local law enforcement officials, local prosecution officials, local educators, private information technologists and mental health professionals throughout the State of Rhode Island. As a law enforcement-oriented task force, their primary goal is to protect children. The ICAC Task Force is charged with the prevention, interdiction, investigation and prosecution of individuals who use the Internet to exploit children. This task force also seeks to combat crimes against children through the Internet by the vigorous investigation and prosecution of offenders.
Website: <https://risp.ri.gov/ccu/icac.php>

Day One RI: 401-421-4100

Provides advocacy support through the RI Children's Advocacy Center and forensic interview; case management and coordination of services (clinical, financial, legal, housing, etc.)
Website: www.dayoneri.org

Child Pornography Victims Assistance (CVPA)

This program responds to investigative requests and ensures that victims can exercise their rights each time their images are included in a federal case. For more information, visit <https://www.fbi.gov/resources/victim-services/cpva>

National Children's Alliance (NCA) When Images Hurt

A guide for non-offending parents on the impact of child sexual abuse images and how to best support their child. For a digital copy, visit <http://csec-response.org/wp-content/uploads/2017/10/NCA-CP-Caregiver-Brochure-smaller.pdf>

HeartMob

HeartMob is a program from iHollaback that creates a community of healing and support for survivors of online harassment.
Website: www.iheartmob.org

PREVENTION & AWARENESS

Enough is Enough

Enough is Enough is a nonprofit organization that focuses on confronting online pornography, child pornography, child stalking, sexual predation, and other forms of online victimization. EIE works on strategies to protect children online.

Website: www.enough.org

Netsmartz

Educational program by the National Center for Missing and Exploited Children; Videos, trainings, handouts and presentations for kids, teens, parents, educators and law enforcement; Various issues such as: sexting, cyberbullying, social media, inappropriate content, and more.

Website: www.missingkids.org/netsmartz/home

Common Sense Media

Nonprofit website with content for parents, educators and advocates including parent guides, classroom curriculum, legislative initiatives and independent reviews from children, parents and experts on apps and other digital content.

Website: www.commonsensemedia.org

Shared Hope International

Shared Hope provides internet safety resources as prevention for child sex trafficking, including guides and webinars for parents and children.

Website: www.sharedhope.org

Internet Matters

Nonprofit website with comprehensive guides on a number of internet safety issues (cyberbullying, online grooming, sexting, etc.) for parents of children of all ages. They also offer advice on buying technology, apps, social media, and online gaming.

Website: www.internetmatters.org

Connect Safely

Nonprofit website with internet safety related tips, advice, guides, news and blogs for parents and educators.

Website: www.connectsafely.org

Protect Young Eyes

Organization that helps families, schools and churches create safer digital environments through faith based and non-faith based presentations, blogs, app/device reviews, and other resources.

Website: www.protectyouneyes.com

REFERENCES

Collier, E. "Parent's Guide to Twitter" (2020) High Speed Training: Hub. <https://www.highspeedtraining.co.uk/hub/parents-guide-to-twitter/>

Common Sense Media. "Parents' Ultimate Guide to Snapchat" (2021) Common Sense Media. <https://www.commonsensemedia.org/blog/parents-ultimate-guide-to-snapchat>

Common Sense Media. "Parents' Ultimate Guide to TikTok" (2021) Common Sense Media. <https://www.commonsensemedia.org/blog/parents-ultimate-guide-to-tiktok>

Common Sense Media. "Twitter" (N.D.) Common Sense Media. <https://www.commonsensemedia.org/website-reviews/twitter>

Cornell Law School. "US Code" (N.D.) Legal Information Institute. <https://www.law.cornell.edu/uscode/text>

Cost, B., Grace, A., Dellatto, M., Hegedus, E. "The 20 Craziest TikTok Challenges So Far - and the Ordeals They've Caused." (2021) NY Post. <https://nypost.com/article/craziest-tiktok-challenges-so-far/>

Facebook. "Facebook Help Center" (N.D.) Facebook. <https://www.facebook.com/help/>

HeartMob. "Twitter Safety Guide" (N.D.) Hollaback. https://iheartmob.org/resources/safety_guides/twitter_guide

Instagram. "Instagram Help Center" (N.D.) Instagram. <https://help.instagram.com/>

Internet Matters. "Instagram Parental Controls" (N.D.) Internet Matters. <https://www.internetmatters.org/wp-content/uploads/parent-controls-docs/parental-control-instagram.pdf>

Internet Matters. "Twitter Parental Controls" (N.D.) Internet Matters. <https://www.internetmatters.org/parental-controls/social-media/twitter/>

Internet Safety 101. "Age-Based Guidelines" (N.D.) Enough is Enough. <https://internetsafety101.org/agebasedguidelines>

Lorenz, Taylor. "How to Prevent 'Zoombombing' in a Few Easy Steps" (2020) NY Times. <https://www.nytimes.com/2020/04/07/style/zoom-security-tips.html>

National Online Safety. "What Parents Need to Know About TikTok" (2021) National Online Safety. <https://nationalonlinesafety.com/guides/what-parents-need-to-know-about-tiktok>

NCMEC. "Is Your Explicit Content Out There?" (N.D.) National Center for Missing and Exploited Children. <https://www.missingkids.org/gethelpnow/isyorexplicitcontentoutthere>

Rodriguez, K. "What is the Silhouette Challenge? A Breakdown of TikTok's Provocative and Dangerous Viral Trend" (2021) Complex. <https://www.complex.com/pop-culture/silhouette-challenge-explained/>

Snapchat. "Snapchat Support" (N.D.) Snapchat. <https://support.snapchat.com/en-US>

State of Rhode Island. "The State of Rhode Island General Laws" (N.D.) State of Rhode Island General Assembly. <http://webserver.rilin.state.ri.us/Statutes/>

Twitter. "Twitter Help Center" (N.D.) Twitter. <https://help.twitter.com/en>

Wamsley, L. "Is YouTube's Algorithm Endangering Kids?" (2017) NPR. <https://www.npr.org/sections/thetwo-way/2017/11/27/566769570/youtube-faces-increased-criticism-that-its-unsafe-for-kids>

