CYBERWORLD

Contains all the important information from our presentation!

Creating a Balance

It can be tempting to consider taking all electronic devices and internet access away from youth for safety, but at heart we know this is not possible. At Saffron, we like to focus on creating a balance between online and offline lives. This includes things like time limits for online activities and encouraging offline hobbies or activities. It also includes thinking about your child's development, what boundaries are in place online, who they are talking to, what they are viewing/playing, how they are being treated online and being aware of their mood and energy offline. Perhaps most importantly, having **open communication** with your youth ensures that if something does go wrong online, they know that you are someone they can go to for help.

Online Parent Resources

MediaSmarts.ca - info about digital and media literacy
HighTechDad - tech reviews
KidsHealth.org - social media and internet safety tips
CommonSenseMedia.org - parent vs. child reviews, conversation starters
TheCyberSafetyLady.com.au - set-up information
ProtectKidsOnline.ca - interests and risks based on age group
GetCyberSafe.gc.ca - info about cyber security
Google - "parental concerns with..." top 10 social media apps
NeedHelpNow.ca - a good resource if you're aware of nude photos that have been posted online that you want removed
CyberTip.ca - can be used to report cybercrimes to police online

TABLE OF CONTENTS

SOCIAL MEDIA & GOOGLE / P. 2-5
GAMING / P. 6-7
SMART HOME DEVICES / P. 7
SEXTING & PORNOGRAPHY / P. 8-9
THE GOOD SIDE OF THE INTERNET / P. 9
WHAT CAN I DO? / P. 10

Virtual Private Networks

What you should know

What is a VPN?

A VPN, or Virtual Private Network, allows you to create a secure connection to another network over the Internet. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.

Why are they useful?

Browsing the internet or transacting on an unsecured Wi-Fi network (such as free public wifi) means you could be exposing your private information and browsing habits. The encryption and anonymity that a VPN provides helps protect your online activities: sending emails, shopping online, or paying bills. This will not only protect your information (credit card numbers, bank passwords) but can prevent hackers from accessing any information youth share online as well.

Sources;
https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/

https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

How do they work?

VPNs essentially create a data tunnel between your local network and an exit node in another location, which could be thousands of miles away, making it seem as if you're in another place. VPNs also use encryption to scramble data when it's sent over a Wi-Fi network. Encryption makes the data unreadable to outside sources trying to look at your information.

VPN Options

- Norton Secure VPN – $4.99-$9.99/mo,
- PureVPN – $10.95/mo
- PVanish – $11.99/mo
- CyberGhost – $12.99/mo
- Hotspot Shield – $12.99/mo
- VyprVPN – $12.95/mo
- Private Internet Access – $9.95/mo
- StrongVPN – $10/mo
- Surfshark – $12.95/mo
- NordVPN – $11.95/mo
- ExpressVPN – $12.95/mo
- TorGuard – $9.99/mo
- Encrypt.me – $12.99/mo
- Safer VPN – $12.95/mo
- HMA – $59.88/year (only annual plans available)
- Tunnel Bear – $9.99/mo

Social Media

What you should know

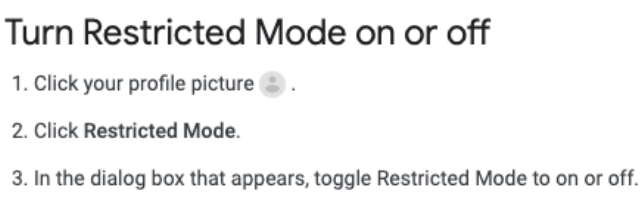
- **You must be at least 13 years old to have an account on any social media platform.**
- **You should only add people that you know on any social media platform.**
- **It's best to turn off Location Services for all social media apps.**
- **Users give permission for these services to store, copy and share any of the content they post.** Every social media platform (YouTube, Instagram, Snapchat, TikTok) includes in their Terms of Service that by using their platform, you grant them a license to use content that you post. They emphasize that you still **own** your content, but the license you grant them is far reaching. This license gives them the power to use, copy, reproduce, process, adapt, modify, publish, transmit, display and/or distribute anything that you post.

YouTube

YouTube is very popular among kids and teens due to the popularity of "YouTubers"; content creators that upload a variety of different entertaining videos. However, it can also be a source of misinformation and inappropriate content. Turning on restricted mode can help by screening out potentially mature content and blocking the comments section on videos. Many youth also want to become YouTubers, which requires creating their own public videos. These videos could be seen by strangers, users may post inappropriate comments on them, personal information might be shared, etc. Have a conversation with your kids about dangers of posting videos online! If they do post, prescreen their videos or make them private so that only people the videos are shared with can see them.

YouTube Kids

If your children are under 13, we recommend using YouTube Kids. While it isn't 100% perfect at keeping out inappropriate content, it has more safety features than YouTube. These features include blocking certain videos, setting up a timer, and search control, which all help in keeping children safer online.



Google

Probably the most popular search engine out there! However, similar to YouTube, it can provide inappropriate search results and can also lead to websites that may be violent, pornographic, or promote unhealthy behaviours. For all devices, we recommend going into Google Settings and turning on Safe Search which will filter out adult content. Recommended search engines for young children include Kiddle, KidzSearch, KidRex, Kid Info, and Quintura.

Twitter

Twitter allows users to share Tweets, messages that can include photos and videos. Users can also like or share other users' Tweets. It's important not to share personal information and be careful what you post on Twitter. Inappropriate tweets have been cited quite often as the cause of public disgrace or job loss. Twitter may also be a source of inaccurate information, so it's important to be critical of what you read. Teach your kids what reliable sources are, e.g. government accounts, verified news outlets, etc.

Instagram

Instagram is an app used to share photos, videos and send private messages. Users can post photos or videos that will remain there until they are deleted by the user. Users can also share via Instagram Stories where their post or livestream can be seen by their followers for up to 24 hours. **Instagram also offers a feature where users can send images that can only be viewed once, similar to Snapchat.** Ensure that youth on Instagram have a private account, which allows them to choose who follows them, and that they know how to filter comments, change message settings, block users and report inappropriate behaviour.

<u>To filter comments:</u>
Go to your profile and tap the three lines in the top right.
Then Tap Settings > Privacy > Comments.
Tap next to Hide Offensive Comments to turn it on.

<u>To change who can send you a message:</u>
Go to your profile and tap the three lines in the top right.
Then Tap Settings > Privacy > Messages.
Select "Only People You Follow" for both options.

<u>To report a user:</u>
Tap the three dots in the top right of the profile.
Tap Report.
Follow the on-screen instructions.

<u>To report a post:</u>
Tap the three dots above the post.
Tap Report.
Follow the on-screen instructions.

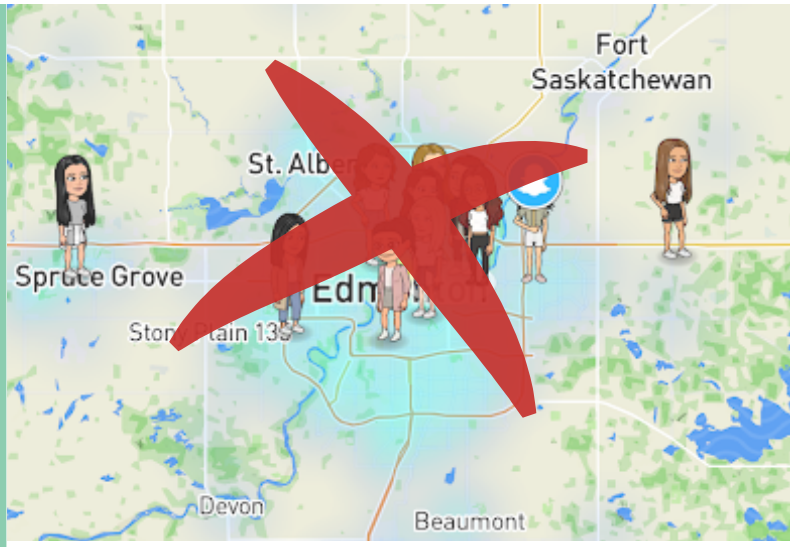
<u>To block another user:</u>
Go to the user's profile that you want to block.
Tap the three dots located in the top right of the profile.
Select 'Block' in the menu that appears
Tap 'Dismiss' on the confirmation message that appears

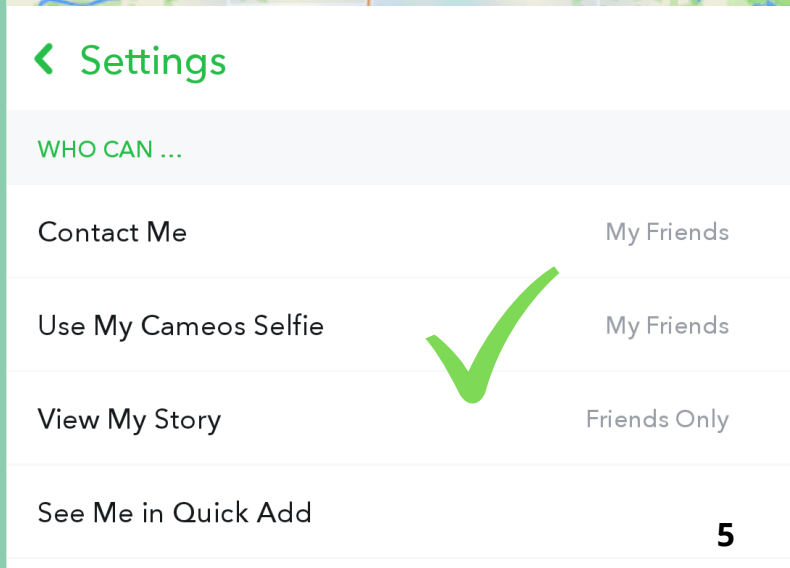
Snapchat

On SnapChat, users can send photos or short videos called 'Snaps'. After being opened by the recipient(s), they cannot look at the photos again, which makes it a popular app for sending nudes. However, you can screenshot any image sent to you and have it saved permanently that way. Stories are posts that are available for 24 hours and can be seen by anyone they have added on Snapchat. If youth send each other at least one 'Snap' per day for a minimum of 3 days, they will have a streak. Kids often give away login info to their friends so their Streaks can be maintained when they don't have internet access. The Snap Map, when enabled, shows the current location of every friend that has the map turned on. This is constantly updated when your kids move around! For safety, it's best to **disable** the Snap Map by turning off location services for the app. Remind youth of the dangers of giving away usernames and passwords. Focus on privacy settings to ensure that only friends can see their account, and pay attention to how they use the app: are they sending/receiving inappropriate Snaps, or looking for pornographic content through SnapChat?

Yolo and Hoop

Snapchat also has two popular add-on apps, Yolo and Hoop. Yolo is an anonymous question-asking app used through Snapchat. The potential exists for bullying, harassment, and other inappropriate behaviours on Yolo. The unfortunate truth is that when people online are given the chance to be anonymous, they often use it to say cruel or hurtful things. Hoop is a way to add new people through Snapchat, and the potential exists for contact with strangers and other inappropriate behaviours. We recommend **avoiding** both of these Snapchat add-ons because of the different dangers that they pose to users.





TikTok

TikTok is a social media app that lets you watch, create and share videos. Because of the app's emphasis on pop music, many videos include swearing and sexual lyrics, which may not be age-appropriate for some kids. TikTok also doesn't have a good filtering system, so scrolling through the app will inevitably lead to viewing inappropriate content. When it comes to posting, the goal of becoming 'TikTok famous' is very common among youth, which leads to having public accounts and copying potentially inappropriate dances or trends in order to try and get more followers and views. Posts on TikTok may become the target of cyberbullying or offensive remarks from strangers if privacy settings aren't enabled. There is also an option to livestream on this app which allows anyone to view the user in realtime. Parents should make sure to turn on all privacy settings for accounts their kids are using. Also, due to lack of filtering and amount of inappropriate content on the app, we suggest that TikTok is only used by ages 16 and up.

Please note: while all the previously mentioned social media platforms can be used by youth with caution, Yubo, Omegle and ChatRoulette are all NOT RECOMMENDED for use in any way. If your youth has been using any of the three platforms mentioned below, it's definitely time to have a conversation!

Yubo

Yubo (formerly 'Yellow') is essentially a dating app for teens; although it markets itself as 'a way to make new friends'. This app allows people to connect with others based on their location, and users ‘swipe’ to accept or decline to talk to someone based on their profile picture. We don't recommend letting any youth use this app, because the potential for being contacted by predators or even other teens with inappropriate requests is high.

Omegle & ChatRoulette

These websites use live video streams and online chat to allow users to talk to strangers. They also advertise their sites as a way to meet new friends. According to a study by RJMetrics, 1 in 8 spins on Chat Roulette resulted in an R-rated experience - a nude individual or an individual engaging in a sexual act. These websites are unregulated and can be home to individuals who inappropriately lure children and youth. All youth should avoid these websites entirely.

Gaming

Check the age ratings for games that youth are playing to ensure that they are age appropriate. These can be found on the physical copy of the game, by searching online, or through app stores. Whether it's violence or sexually explicit material, the content can influence their thoughts and behaviours. It can also be helpful to read reviews before deciding to purchase specific games. **CommonSenseMedia.com has age ratings, reviews, and spots for parents to share their thoughts.** It is also essential to talk about privacy settings with your youth. These settings control who can contact them, and it's best if only friends can do so. Computer games will have different settings within each game and distribution service (Steam, Blizzard). Be sure to turn off the location settings of any gaming consoles (xBox, PS4) and set parental controls for them, so you can change settings and view the history. It is also a trend to livestream yourself playing games on Twitch. Talk to your youth about the dangers of livestreaming - unintentionally sharing personal information, getting contacted by strangers, etc.

What Else to Consider

- **Be aware of emotions** – cyberbullying and harassment are a growing problem in online games. Pay attention to how they seem when they are on and offline (e.g. withdrawn, angry, sad, etc.)
- **Stay informed** – search the internet for popular new games, and any issues that have been reported with those games. And stay up to date on the kinds of games **your** kids are playing so you know what to look out for!
- **Play with them** – this may not be something you want to do, but getting involved in their gameplay ensures you approve of what they play and you can get a glimpse into what gaming is like for them.
- **Stranger danger** – one of the main problem with games is communication with strangers. Cautioning against talking to strangers, encouraging only playing with friends and muting others and themselves will all help to keep them safe.
- **Open communication** – and as with all things, we stress open communication! Do your best to make sure your kids feel comfortable coming to you if they run into any inappropriate behaviour.

Discord

Available now on PC, Xbox and will soon be available on PS5

Discord is a voice, text and video chat service that's used by gamers to communicate with others while they are playing together. The chatrooms on Discord are called servers, and they can be private or public. Users can join a chat they've been invited to or they can create private servers and invite their friends to play and discuss games. Issues with Discord are often around the topic of discussion in servers., e.g. cyberbullying and harassment. A shift in mood after gaming might be a sign that they were involved in harmful discussion. However, there are also a number of features of Discord that make it safer for kids. Private servers can be restricted to users with an invitation code, and users need to have the username and a 4-digit tag number of another user in order to become "friends". All chatrooms are opt-in, so anyone not interested in chatting has a number of tools at their disposal. E.g. unwanted or inappropriate users can be blocked and muted. There are also parental controls including an explicit content filter, direct message scanning, ways to block unwanted messages or friend requests.

Smart Home Devices

Smart home devices can range from security cameras to controlled lighting, but we are focusing on voice activated assistants, such as Google Home and Amazon Echo. After you activate these devices, all your questions and requests are recorded and saved by the company. This is for quality control and the improvement of the service, but important to know regardless. These devices can also fail to interpret your voice accurately. For example, a woman's Amazon Echo recorded a private conversation and sent that recording to people on her contact list because it thought it heard the wake word, a send message request and interpreted background noise as a contact's name. If you don't want your kids to be able to use voice activated assistants, including Siri on iPhones or other personal devices, you can disable the microphone in Settings. New smart home devices often have a switch to disable the microphone directly on the device. You can also block restricted content, such as explicit music and videos, by enabling filters on your device. Do an online search for "filter for [device name]" and results will show step-by-step instructions on how to enable these filters.

Sexting & Pornography

Sexting is the sending nude or semi-nude photos via an electronic device. Why would someone sext? There's a number of reasons why someone might sext another person. Pressure to fit in, because they believe it's normal, and/or because of harassment. If youth are constantly getting texts, calls, or even being approached in person about sending sexts, they might send a photo not because they want to, but to get the other person to leave them alone. Harassing an individual for nude photos is always unacceptable. And anyone under 18 shouldn't send these sexts for any reason because it is **illegal** under the Canadian Criminal Code. Note: the police recommend that if your child has been sent an **unsolicited** sext, to SAVE the image (so it can be used as evidence) and then take it to them IMMEDIATELY for investigation. Talk to youth about the realities and dangers of nude photos.

Criminal Code Section 163.1

Taking, sending and saving nude or semi-nude photos or videos of someone under the age of 18 can result in child pornography charges. And parents/caregivers are often the owner of youth's cellphones, so they can be held accountable for the content of their youth's phones.

Bill C-13

It is also illegal to share intimate photos of ANYONE (regardless of their age!) without their consent, and you can face up to 5 years in prison for this. Why such a hefty charge? Because of the effects it can have on victims, which can include depression or even suicide.

Did you know?

"About four in 10 young Canadians have sent a sext and more than six in 10 have received one . . . and about 40 per cent said at least one of their intimate photos had been shared without their consent."

Source: https://globalnews.ca/news/4010783/new-report-shines-spotlight-on-young-canadians-sexting/

Be aware of apps that can hide photos:

1. KeepSafe Photo Vault
2. 1Gallery
3. LockMyPix
4. Calculator by FishingNet
5. Vaulty
6. Hide Something
7. Vault
8. GalleryVault
9. Androgynito
10. PhotoGuard

Sexting & Pornography

Watching porn leads to changed perspectives regarding sexual relationships, especially at a young age when the brain is still developing. It's possible to develop an addiction and 'get used' to pornography, which can result in seeking out more intense pornography in order to elicit the same response. The way that sex is portrayed in pornography is not realistic, and not a depiction of a healthy sexual relationship! There can be situations where partners try and attempt what they see in porn in their real-life sexual relationships, which can include physical violence and emotional abuse. How can you approach youth about pornography? It's not an easy conversation to have, but it is important.

Reduce shame: shame causes many teens who are struggling with pornography to be hesitant to answer questions. Minimize shame by being non-judgmental and supportive about their struggles.

Normalize the issue: reassure them that seeing pornography is common while also communicating the dangers it can have.

Be open: have honest discussions about sex, emphasize that porn is not a depiction of a healthy relationship, and talk about the importance of respect and consent in relationships

The Good Side of the Internet

Please keep in mind that the Internet is not all bad! Technology is an instrumental part of all our lives, and it can be a positive addition for children and youth. The Internet allows them to discover new topics, areas of interest and connect with friends and family. It also provides a wealth of information and resources for learning about important social issues. All this information helps with expanding minds and prepares youth for the future. Technology is also something used in many professions. Gaining familiarity and proficiency in their younger years is great preparation for future careers. Additionally, social media allows for networking, which creates connectivity, belonging and opportunities for support. It's all about balance. Teach your kids how to use the internet in a useful way; playing educational games, reading informative websites, and following positive people on social media.

What Can I Do?

Get Involved!
Whether they're on social media, playing games or watching videos. It will allow you to see what they are doing and is a starting point for open communication, because they know that you're a part of their online life. It might also make them more likely to come to you with problems if they know you are familiar with their online activities.

Don't be Afraid to Intervene
Tell youth about red flags, such as someone asking for or sending intimate images, bribes and unusual gifts, threats and intimidation, or any behaviour that makes them feel uncomfortable. Let them know to speak to you if they hear or see anything suspicious. Tell them and show them that they can trust you.

Contact Us!

Have any questions or comments?
Feel free to reach out!

Email:
publiced@saffroncentre.com

Phone:
780-449-0900

Communicate with Youth
Be sure to set clear expectations for device usage early on. These expectations can be set well before they receive an electronic device. You and your youth can agree on time limits, when they can use it, where they can use it, what sites or apps they can use and what is considered inappropriate. You can also mention how you will regulate their behaviour. You may agree on spot checks and/or filtration and monitoring devices. It is important to involve them in the conversation! It is also essential to talk to youth about healthy relationships, boundaries, online bullying, pornography, and the consequences of sexting. Talk about the permanency of their posts online. Inform them that all of their posts, pictures, likes, and shares can be viewed and used to determine their candidacy for a job, school, or volunteer roles.

Listen to Youth
Get involved in youth's discussions about the internet. Use it as an opportunity to gain knowledge about the apps they use and the games they are playing. Pay close attention to the details! They can help you in future discussions. Be sure to also listen for any issues they may be having and how they are feeling online. Do they have anxiety online? Are they facing peer pressure? Do they vent anger or frustration online? Do they know when they need parental help? These are all great conversations to have!

Set Aside Tech Free Time
Consider implementing this rule for kids **and** parents: no devices 1 hour before bedtime. Setting aside even more tech-free time can also allow your family to spend more time together and build a stronger bond. Try some offline family activities!

Think about the age they get their first device.
Many parents want their young children to have devices so they can contact each other in case of emergency. Be mindful about other apps and games the device can be used for, and if they are age appropriate.