WHAT EVERY PARENT SHOULD KNOW TO KEEP THEIR CHILDREN SAFE ONLINE

Teaching Parent’s Social Media Literacy

Abstract

Teaching parents’ social media literacy involves empowering them to guide their children in critical thinking, privacy management, and responsible online behavior through open conversations, modeling good habits, setting boundaries, and using tools like parental controls, focusing on building trust so children feel safe discussing online experiences and potential risks.

Compiled: 20 January 2026

By: Glen Hutton

for the

Vulcan COUNTY
Health & Wellness Foundation

VULCAN COUNTY
MENTAL
WELLNESS
COALITION

CONTENTS

TEACHING PARENTS' SOCIAL MEDIA LITERACY

- Teaching parents' social media literacy involves empowering them to guide their children in critical thinking, privacy management, and responsible online behavior through open conversations, modeling good habits, setting boundaries, and using tools like parental controls, focusing on building trust so children feel safe discussing online experiences and potential risks.
- Key areas include understanding data privacy, recognizing misinformation, assessing source credibility, interact responsibly online, and practicing empathy to navigate digital citizenship effectively.

CORE PRINCIPLES FOR PARENTS

BE A ROLE MODEL:

- Practice what you preach by managing your own digital footprint responsibly.

FOSTER OPEN COMMUNICATION:

- Talk weekly with your kids about their online lives without judgment to build trust and encourage them to share concerns.

TEACH CRITICAL THINKING:

- Help kids question what they see online, understand media influence, and evaluate source credibility.
- Help kids understand that not everyone they meet online is who they say they are.
- Teach them to never accept 'friend requests' from people they don't know in real life; online "friends" can be strangers.
- Help your children understand that any photos, videos, or text messages can be permanent and others can share them with anyone.

PRIORITIZE PRIVACY:

- Teach them to limit personal info, use strong passwords, customize privacy settings, and understand that "temporary" posts aren't truly gone.
- Teach them to never share their full name, address, phone, school, or photos without parent permission.
- Teach them to keep passwords private, even from best friends, and only share them with parents.

SET CLEAR BOUNDARIES:

- Establish rules for screen time, device locations (e.g., no phones in bedrooms), and age-appropriate content.
- Help them understand that posting mean messages about other people is wrong. Remember treat others as you would like to be treated.
- Ensure they understand that they must have your permission before downloading and installing apps.
- Teach them that should never click on any link without your permission.

PRACTICAL STRATEGIES FOR PARENTS

DIGITAL CITIZENSHIP LESSONS:

- Discuss empathy, respect, responsible online behaviours, and the consequences of online actions, using real-life examples.

USE PARENTAL CONTROLS:

  - Utilize built-in settings on devices, apps, and search engines to filter inappropriate content.

EXPLORE TOGETHER:

  - Browse websites and apps with your children to understand their digital world firsthand.

ADDRESS RISKS PROACTIVELY:

  - Discuss threats like cyberbullying, predators, and misinformation, and teach kids how to report issues.

FOCUS ON PRIVACY SETTINGS:

  - Regularly review and customize privacy settings on all platforms together.

By teaching these skills, parents move beyond just monitoring to actively equipping children to thrive safely and responsibly in the digital world and building digital literacy as a key life skill.

HOW KIDS USE SOCIAL MEDIA

https://caringforkids.cps.ca/handouts/behavior-and-development/social_media

KIDS USE SOCIAL MEDIA IN MANY DIFFERENT WAYS

- **Communication:** Messaging, commenting, chatting with friends and family, even those far away.
- **Entertainment:** Watching short videos (TikTok), funny clips, following influencers, finding memes.
- **Content Creation & Sharing:** Posting selfies, photos, videos, creating music, sharing crafts, remixing content.
- **Information & Learning:** Discovering educational content, news, tutorials, or information about hobbies.
- **Identity Exploration:** Trying out different personas, finding communities with shared interests (e.g., gaming, art).
- **Socializing:** Seeing what friends are doing, participating in trends, feeling connected, and escaping real-life issues.
- **Gaming/gambling:** Some gaming apps include online gambling, and many feature product promotion or advertising.
- **Online dating:** Although most dating sites/apps are for people over 18 years old, many do not require proof of age. Users can be manipulated by others to share personal information and inappropriate photos.

BENEFITS

STRENGTHENS BONDS:

- Helps maintain real-life friendships and family ties.

BUILDS COMMUNITY:

- Connects kids with peers who share niche interests, especially if they lack local connections.

FOSTERS CREATIVITY:

- Offers platforms to share talents and learn new skills.

PROVIDES SUPPORT:

- Can be a source for mental health info or support groups.

RISKS OF KIDS USING SOCIAL MEDIA

CYBERBULLYING:

- Online harassment can be severe and harmful to mental health.

SEXTORTION (A BLEND OF "SEX" AND "EXTORTION"):

- Is a serious cybercrime where a perpetrator uses sexually explicit images or videos to blackmail a victim. As of 2026, it is recognized globally as a form of image-based sexual abuse.

HARMFUL CONTENT:

- Exposure to inappropriate content, extreme ideas, or dangerous behaviors (like substance use). Examples include **the Manosphere, online misogyny, gang recruitment, online drug sales.**

PRIVACY & SAFETY:

- Oversharing personal info, location, or private details.

MENTAL HEALTH:

- Social comparison, body image issues, pressure for likes, and anxiety.

SELF-ESTEEM:

- Being able to see what friends are doing in real time—especially if your child has been excluded —can affect self-esteem.

ADDICTION:

- Social media apps are designed to keep people online as long as possible. Constantly checking for “likes”, followers and messages can lead to unhealthy behaviours and mood changes.

PARENTS CAN MINIMIZE THE RISKS

- Learn about the apps your child is using. While some social media platforms have age requirements to join, children may get around these.
- Show interest and ask questions about your child’s online experiences. Make sure they understand that it’s not a good idea for adults to communicate with children and teens online.
- Try to keep tablets and computers in common areas where you can monitor your child’s use. Keep devices out of private spaces like bedrooms.

- Get online family protection. Programs that provide parental controls can block websites and enforce time limits. Talk to your kids about ways to keep from seeing things they don't want to see, like setting filters on search engines (your child is probably more interested in avoiding inappropriate content than finding it).
- Be open with your children if you are following their online accounts or monitoring their online activity to help keep them safe. Because some children or teens may create a fake second account for their parents to follow, ongoing conversation is essential.
- Discuss what's okay and safe to post online, and what isn't. Talk about how privacy settings or other tools can control who sees what they post, and what they might do if the wrong people see their content.
- Find the app's "safety centre" or "parent centre" and go through it with your kids (if you can't find it within the app, do a Google search with the app's name and the words "safety centre" or "parent centre"). These features have information about limiting what people can see and how they interact with you, as well as what to do if things go wrong.
- There is a strong relationship between having rules in the home and how kids behave online. Talk with your kids about: what information they post/share and how they "talk" online; how/whether to comment on others' posts; speaking up when something feels wrong or uncomfortable.
- Make sure your kids know that they should come to you if anything ever goes wrong or upsets them online. Tell them that your top priority will be working with them to fix whatever's gone wrong.
- Remind your children that what they see on social media doesn't always reflect reality and help them find joy in offline activities. If you see your children getting anxious about being off their phone for a while, talk about how they are feeling.
- Set a good example by following the rules you set for online behaviour. Ask them before you share anything about them

ONLINE PRIVACY

- Most social media apps and websites have privacy policies and settings, but they are all different.
- Start by getting familiar with the apps themselves:
    - Read an app or website's privacy policy before sharing any personal information.
    - Check this website for plain language summaries of popular apps' policies.
    - Check your child's privacy settings and profiles to make sure they aren't sharing identifying information such as their birthdate or location.
    - Most apps require users to set up a profile, which can include name, e-mail address, birthdate, phone number, interests, and a photo. Depending on a user's privacy settings, some profiles are visible to the public, while others can only be seen by friends or followers.
        - Whenever possible, encourage your child to use an online nickname, instead of a real name.

- If your child uses a GPS-enabled smartphone or tablet, they could be posting status updates, photos and videos with “geotags”.
    - Geotags share the exact location of where a photo was taken. Turn off these features.
- If your child uses an iPhone or an iPad, you can keep apps from tracking them by tapping Ask App Not to Track when you download it.
    - For apps you’ve already downloaded, go to Settings → Privacy & Security → Tracking, and slide Allow Apps to Request to Track to off.
- For Android phones or tablets, download the DuckDuckGo app, go to Settings → App Tracking Protection and slide to on.

TEACH YOUR CHILD HOW TO PROTECT THEIR PRIVACY

- Never accept friend requests from people they don’t know in real life.
- Keep every account password protected, and change passwords often. Do not share passwords, even with friends.
- Remember that no matter what the app says, posts are not temporary. People can take screenshots of a photo before it disappears.
- Protect and respect their friends’ privacy by asking permission before posting a photo or video of another person.
- Know what their friends are posting about them.

Empowering families to navigate the digital world safely requires a combination of digital literacy, open communication, and proactive parenting.

By teaching our children digital literacy skills, setting clear boundaries, and fostering critical thinking, we equip them to make informed choices and protect their online well-being.

Remember, promoting online safety is an ongoing process that requires adaptability and vigilance.

By staying engaged, informed, and supportive, we can help our children harness the potential of the digital world while minimizing its risks.

PRIVACY TIPS FOR PARENTS AND CAREGIVES

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/tips-for-parents/online-tips/

12 ONLINE PRIVACY TIPS FOR PARENTS AND CAREGIVERS

- Raising kids in a digital environment presents new considerations and challenges. Young people today are using technology effortlessly and easily adapt to new connected devices. Online tools are a routine part of children’s lives, as they use them to chat, post, play and learn.
- Many kids, however, do not fully understand the impact that some online activities may have on their privacy. Below are 12 tips to help you empower your children with knowledge about the implications of their privacy choices and allow them to make the most of their time online, safely.

1. TALK TO YOUR KIDS

- It is important to know the online spaces that your kids frequent and the devices they use to go online, to help you understand the nature of personal information that they may be sharing.
- Ask your kids what they like about the services and online spaces they are accessing to start the conversation.
- Technology changes rapidly and many children are ahead of adults in adopting new tools.
- By talking frequently, you will gain more insight into their activities online and any potential benefits or risks they may be facing.
- If your children are under 13, explain that age limits for services exist for good reason, and accessing services that are not intended for them could lead them to harm. It’s not a good idea to lie about their age to create accounts on websites that are designed for or restricted to older children and adults.

2. TRY IT OUT

- It is not enough to know what online spaces and devices your kids are using. To understand the nature of the personal information they are sharing, you should know how they are using and experiencing them.
- So, dive in. Play the online games they love, create a profile on the social media platforms they frequent, and download some music.

3. KEEP UP WITH THE TECHNOLOGY

- Many mobile devices, like smart phones, tablets and gaming consoles, can connect to the web and have video cameras.
- The lines between devices are blurring, and it is important to know what kind of device your child has, so that you know whether they are merely playing a game, or if they are using the Internet and sharing personal information.
- You could also do some research online about the technologies they are using if you are concerned about safety, including risks to privacy.

4. WALK THROUGH ACCOUNT SIGN UP AND PRIVACY SETTINGS TOGETHER

- If your child is just learning about how to create accounts, go through the sign-up steps together and discuss how the information they are posting could be used – or misused – by others.
- If an email address is required, consider creating one that is just used for apps or for specific types of services, such as for gaming.
- Where needed, set parental controls. Most social media sites have privacy settings options that children should learn to use. Review how personal information will be collected and used and the options for limiting the sharing of personal information.
- Depending on your child's capacity, modify the privacy settings yourself, or modify them together.
- See our tips for using privacy settings.

5. MAKE PASSWORD PROTECTION A PRIORITY

- Children need to understand that their online information will be better protected if they use strong passwords. They should use unique passwords for each different website, account and device.
- Encourage them to ensure their passwords are strong (15 characters or more and a variety of letters and/or numbers).
- See our tips for creating and managing your passwords.

6. EMPHASIZE THE IMPORTANCE OF PROTECTING MOBILE DEVICES

- The first thing anyone should do with a new mobile device is activate the password protection.
- Talk to your kids about this, and the importance of protecting the device itself – not just because it may be expensive, but because it may contain their personal information.
- A device that gets into the wrong hands could result in embarrassing or even malicious videos or pictures being posted online by someone else in your child's name.
- Learn more about protecting personal information on your mobile devices.

7. REMIND YOUR KIDS THAT WHAT THEY POST ONLINE IS NOT ALWAYS PRIVATE

- Your kids should understand that once they post content online, they may no longer have control over it. It can be forwarded, copied and pasted, manipulated, printed out or saved – it can remain online, in some form for a very long time.
- Even password-protected pages are not totally secure, and that deleting information does not mean that it is gone forever.
- You could also tell them that social media companies collect and use their posts and online activity for purposes such as advertising.
- Many young people are not aware that their personal information is being collected and used in this way. Information on how their personal information is being collected and used is explained in the service's privacy policy.

8. TEACH YOUR KIDS TO THINK BEFORE THEY CLICK

- It can take only seconds to snap a photo and post it online, or to post a comment. But it can be very difficult to permanently delete that comment or photo once it is posted, as it can then be downloaded or archived by others.
- This is why it is so important for kids to think twice about every piece of personal information before they post it online.
- They should only post things that they would be comfortable with the whole world seeing.
- They should also ask permission before posting things about other people.

9. STRESS THE IMPORTANCE OF KNOWING YOUR REAL FRIENDS

- Kids need to know that, online, they cannot be 100% sure of who they are talking to, so they should never accept friend requests from people they do not know in real life.
- Online friends can end up accessing online photo albums, reading personal comments, copying and pasting information, knowing what you are doing and where you are.
- Remind your kids that a "friend" of a "friend" of a real-life friend is really just a stranger. For more information, see our advice, are your online friends who they say they are?

10. TEACH YOUR KIDS THAT THEIR PERSONAL INFORMATION IS VALUABLE

- Kids need to know that many people and companies want their personal information to sell or market things to them in the future. New and exciting technologies are emerging daily, but often personal information is the cost of admission.
- Review the personal information they often need to surrender in order to play online games, fill out an online survey or quiz, join virtual worlds or even just shop online.
- Discuss ways to limit that information, for example, by completing only required fields, using pseudonyms, and using incomplete information.

11. LET YOUR KIDS KNOW THAT YOU ARE THERE IF THEY MAKE A PRIVACY MISTAKE

- Stay calm if your child makes a mistake, like posting something they should not have. Help them remove the post, where possible, and talk with them about how they can avoid a similar mistake in the future.
- If you "freak out" or deny access to them, they may not come to you for help when they really need it in future.
- See our information on privacy and sexting.

12. SET A GOOD EXAMPLE

- Remember, those funny back-to-school pictures of your own child that you are tempted to post can also be copied and shared and remain online for a very long time!
- Just as you would respect your friends when posting photos or other items that contain their personal information, respect your kids' personal information too.
- Set a good example when you are online, so your kids have a good role model to look to if they are wondering what kind of information is okay to post.

SHARENTING

ARE YOU SETTING A GOOD EXAMPLE FOR YOUR CHILDREN?

- **Sharenting" or "oversharenting"** are relatively new terms that combine the words "oversharing" and "parenting" to describe the actions of those who often post about their children or grandchildren's lives on public social media platforms.
- Online public platforms, such as Facebook, X, Instagram, and Reddit, allow users to share content (text, photos, videos) intended for broad public access, forming digital communities and spaces for information sharing,
- In Canada, sharenting (oversharing photos and information about children online) poses significant risks to a child's privacy, safety, and future well-being.
    - These risks range from immediate threats like identity theft and image exploitation to long-term psychological and social consequences.
    - Posting a photo or video can have serious consequences for your child. For example, it could affect their reputation, dignity or self-esteem.
    - Taken out of context, images of their daily life could expose them to ridicule and cyberbullying.
- As your child ages, they may also feel uncomfortable with the knowledge that images of them have circulated on social media.

KEY REASONS WHY YOU SHOULD NOT UPLOAD IMAGES TO ANY PUBLIC SOCIAL MEDIA PLATFORM

LOSS OF CONTROL AND OWNERSHIP:

- Once a photo is uploaded to a social media platform, the user often grants the platform a license to use, distribute, or even sell that content to third parties.
- Even if you delete the post later, the data may remain in archives or have been saved by others via screenshots.

AI EXPLOITATION AND DEEPFAKES:

- As of 2026, generative AI can easily "scrape" publicly available photos to create realistic deepfakes or nonconsensual imagery.
- Some AI companies use online photos of children as training data for facial recognition without parental knowledge.

IDENTITY THEFT AND FRAUD:

- Posting personal details like a child's full name, birthdate, or location (e.g., in front of their school) provides data that malicious parties can use for identity fraud, even years later.
- **Security experts predict that by 2030, a significant portion of youth identity fraud cases may stem from parental oversharing.**

IMAGE EXPLOITATION:

- Innocent photos, such as those of children in swimwear, can be downloaded, circulated, and misused by pedophiles on the dark web or child pornography sites.
- Technology also allows for the creation of sexually explicit "deepfakes" using a child's image.

PRIVACY BREACHES:

- A child cannot give informed consent to having their entire life documented online, creating a permanent digital footprint before they are old enough to understand the implications.
- Privacy settings offer limited protection, as anyone with access can screenshot and re-share images outside the intended audience's control.

PSYCHOLOGICAL AND SOCIAL HARM:

- Children may feel embarrassed, anxious, or betrayed by photos posted without their permission.
- These posts can lead to bullying or cyberbullying and potentially impact their future opportunities, such as employment or university admissions.

VULNERABILITY TO PREDATORS:

- Revealing routines (like a photo in a school uniform) or locations through geotagging can provide information to online groomers or other malicious individuals, compromising the child's physical safety.
- Predators often scour social media for images of children. Even innocent-looking photos can be misused or shared on harmful forums. Approximately 50% of photos shared on such sites were originally posted online by parents themselves.

THE CANADIAN LEGAL CONTEXT

The Canadian legal framework surrounding sharenting is still evolving, but experts point to several key considerations:

PARENTAL CONSENT:

- In Canada, parents and guardians are currently responsible for exercising their children's rights and providing consent for data sharing.

CHILD'S RIGHT TO PRIVACY:

- While children have a right to privacy, they have little recourse under current social media policies to make content disappear once it's online.

"RIGHT TO BE FORGOTTEN":

- Unlike some European laws (GDPR), Canada does not currently have a federal "right to erasure" law that would allow individuals to demand their personal data and images be deleted when they reach adulthood.

SHARENTING BEST PRACTICES

Canadian organizations like ProtectKidsOnline.ca recommend that photographs of your children should never be posted on open, public social media platforms.

THINK BEFORE YOU POST:

- Consider how your child might feel about a photo in 10 years.

OBTAIN CONSENT:

- If the child is old enough to understand, ask for their permission before posting.

LIMIT INFORMATION:

  - Avoid sharing identifiable details such as their full name, school, location, or birthdate.

USE CAUTION WITH PRIVACY SETTINGS:

  - Set social media profiles to private but recognize that even private settings are not foolproof.

BE A GOOD ROLE MODEL:

  - Teach your children about online privacy by modelling responsible sharing behaviours.

For more information and resources, parents can consult with organizations such as the Office of the Privacy Commissioner of Canada and

ProtectKidsOnline.ca