Helping our kids
use their smartphones safely

Created in partnership with:

Media Smarts

GETCYBERSAFE.CA
Protect while you connect.

TELUS

Helping our kids
use their smartphones safely

Welcome note from Andrea Goertz

If you have a school-age child, you've probably been asked this burning question already: "Can I have a smartphone?" Making the decision on when it's the right time is a giant hurdle in itself, but keeping them safe online can seem like a never-ending challenge.

As a mother of two teens, I see the benefits every day of my children and their friends interacting with technology, whether it's on a smartphone, tablet or laptop. It can be a highly positive experience when it comes to social connection, education and family communication. However, as parents, we need to understand the power of smart devices and the opportunities they bring so we can confidently guide our kids when they're ready to get their first device.

This is why we have created this guide; to help all parents make an informed decision.

We believe in the power of communities coming together to accomplish great things, so TELUS WISE, TELUS' unique educational program focused on Internet and smartphone safety, has teamed up with Get CyberSafe and MediaSmarts. Through our partnership, we have created this easy-to-navigate guide for parents and caregivers to learn how to positively empower children about online safety when they're starting to use technology.

Since launching TELUS WISE in 2013, we have reached more than 750,000 Canadians through free seminars and online resources dedicated to help keep all members of Canadian families safer online. I hope you find this new guide for parents helpful and valuable. If you have any questions, please contact us at wise@telus.com

Regards,

Andrea Goertz - Executive sponsor of TELUS WISE
Chief Communications and Sustainability Officer, TELUS

1. What are kids doing online?

Media Smarts
YOUNG CANADIANS IN A WIRED WORLD

Life Online

Canadian students are more connected, more mobile and more social than ever.
www.mediasmarts.ca/YCWW

ONLINE ACCESS

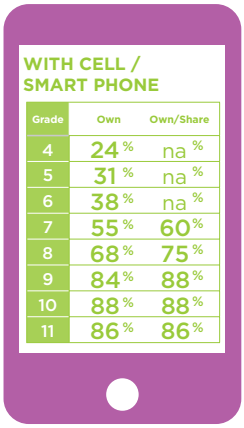
45% of students access the Internet using a cell/smart phone

60% of boys access the Internet through a gaming console

GRADE	Shared Desktop	Own Desktop	Portable Computer	Library or Community Centre	MP3 Player	Cell / smart phone	Game console
4	64%	17%	56%	6%	47%	12%	46%
5	59%	19%	62%	9%	49%	21%	47%
6	59%	20%	63%	6%	55%	25%	48%
7	54%	21%	69%	7%	55%	37%	45%
8	50%	23%	73%	4%	53%	56%	41%
9	41%	23%	75%	6%	44%	68%	43%
10	39%	25%	78%	6%	38%	69%	34%
11	37%	27%	73%	6%	36%	75%	38%

59% of kids grades 4-11 have their own cell phone (smartphone or cell phone without data capability).

69% have access to a cell phone (their own or someone else's).



CRUEL OR MEAN BEHAVIOUR

55% of students who participate in mean or cruel online behaviour say they were "just joking around".

Retaliation is another common reason:

48% said it was because someone said something mean or cruel about them first.

32% said it was because someone said something mean or cruel about one of their friends first.

RESPONSES TO CRUEL OR MEAN BEHAVIOUR AND THREATS

Ask parent(s) for help	50%
Ignore it and hope it will go away	42%
Ask friends for help	38%
Ask a teacher for help (9th on a list of 11 options)	17%

Students are more willing to rely on face-to-face communication to deal with conflict.

BYSTANDERS AND INTERVENERS

65% of students have done something to help someone who is being picked on online. Students who have been cyberbullied and those who have cyberbullied others are both more likely to step up and help.

SCHOOL CULTURE, RULES AND INTERVENTIONS

There is little correlation between having school rules and whether or not a student has **engaged in** or been the **recipient of** cyberbullying. However, having a rule at home that you must treat people online with respect correlates with lower levels of mean or threatening behaviour.

LEARNING ABOUT CYBERBULLYING

62% of students have learned about cyberbullying from teachers

43% from their parents.

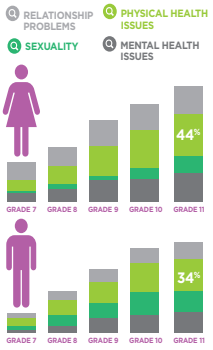
ONLINE ACTIVITIES

THE MOST FREQUENT ONLINE ACTIVITIES REPORTED BY STUDENTS ARE:

52% of kids in grades 4-11 read or post on social networks once a week or more

Among grades 4-6 students, **32%** have a Facebook account

Among grades 7-11 students, **82%** have a Facebook account



METHODOLOGY

Conducted February to June of 2013

5,436 Canadian students in grades 4-11 in 10 provinces and three territories

41% boys | 46% girls | 13% no indication

126 English | 14 French

140 schools in 51 school boards

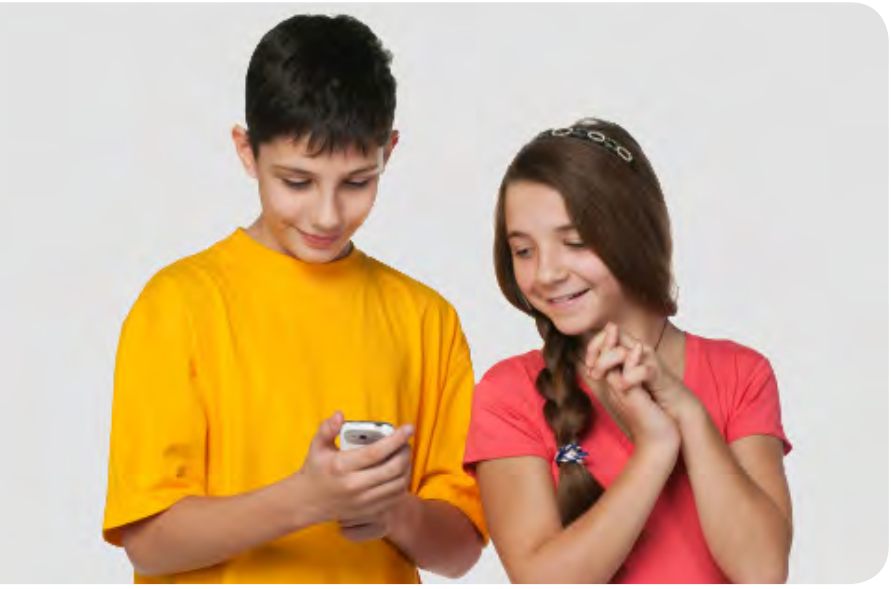
Source: **MediaSmarts**

2. Is your child ready for a smartphone?

A frequently asked question is ‘What age should my child be before I get them their first smartphone?” The answer is not so much about the age of the child but rather their maturity and ability to use their smartphone responsibly. Ask yourself these questions to help with the decision in getting your child their first smartphone:

- Have you set limits for the use of iPods, tablets, computers and game consoles? If yes, does your child understand and respect these limits?
- Does your child need a phone to stay in contact with you in case of an emergency?
- Can your child be trusted not to use the phone during inappropriate times? (e.g. in class)
- Have you laid the foundation for responsible smartphone behavior and talked with them about sharing inappropriate pictures and posts?

When you can answer ‘yes’ to all of these questions, you’ll know that your child might be ready for their first phone. It doesn’t stop here, you need to keep the conversion going about appropriate online behavior with your child – whether they are using a smartphone, tablet, computer, network game council or iPod.



3. Once you have made the decision to give your child a smartphone

Okay, you have made the decision to give your child a smartphone, which they can't wait to get in their hands. Here are some things to think about before you purchase the phone.

Before purchasing a smartphone for your child

Consider these factors:

Device restrictions: Not all devices are created equal when it comes to parental restrictions. Before purchasing a smartphone do your research into which restrictions are available on current models of smartphones and decide which one makes the most sense for your family.

Data versus voice only: Decide whether you want your child to make calls only or also have data capability – which will allow them to text, email and surf the Internet. Also talk to your service provider about data plans and how you can manage their data usage/consumption.

Form versus function: While there are some great looking smartphones on the market that have a lot of features, before you make a decision on the smartphone you purchase think about the functionality and durability of the phone when in your child's hands.

If you are giving them a used family phone: Another option is to give your child your existing cell phone and acquire a new one for yourself. If you do this make sure you do a complete wipe of all of your data before handing over the phone.

Before you hand over the smartphone to your child

Before handing over control of the phone to your child there are a few things you can do, along with your child, to make sure they get the most out of their smartphone – safely and responsibly. We have broken these out into the following categories:

a) Safety first

b) Data usage

c) Social media and applications

d) Other important considerations

a) Safety first

Set up lock function. Probably the most important step is to set the lock function on the phone and change the settings to lock the screen automatically after 1-5 minutes. Locking the screen is a particularly important step for kids with smartphones as "friends" can pick up each other's phones and as a "joke" post comments on their Facebook accounts (which kids often leave logged in) or send troublesome texts or emails pretending to be the owner of the phone.

Set strong passwords. Set a strong password on the smartphone, apps and social networking accounts (e.g. Instagram) that your child belongs to. A good password can help stop someone from hacking into their smartphone, social networking accounts or changing passwords on their applications. A good password is at least six characters (numbers, letters, etc.) long. You can make your password stronger by using the first letters of a phrase, instead of a word — ICARMLP for "I can always remember my laptop password", for instance — and changing some letters into numbers or other characters. Ensure your child has strong passwords, and is not using the same password across multiple accounts. Also ensure your child knows not to share their password with anyone except for you.

Install and/or activate remote locate/lock/wipe software and install security software. Free software is available for you to download onto your phone that will lock, track or remotely erase the information on your phone if it is lost or stolen. For the iPhone it's called Find my Phone, for the Blackberry it's Blackberry Protect and for Android phone it's different for each manufacturer. For example, Samsung has what's called a Mobile Tracker.

Ensure geo-tagging is turned off. Photos or videos taken from most smartphones include a geotag – the exact location of where the picture has been taken. Think of it this way – if your child takes a selfie of their first day at school and shares this picture or posts it to their favorite social networking site anyone can find the exact location of where this picture is taken. Geotagging is usually a camera setting or general setting on the phone.

Add family and emergency contacts to the contact list. Add parents, grandparents, sitters and I.C.E. (In Case of Emergency) contacts. Having a few contacts labeled ICE lets anyone know who to call in case of an emergency.

How to handle emergencies. Make sure your child is aware that they can and should call you and/or dial 9-1-1 in an emergency.

Teens and driving. More than one-third of Ontario teens have admitted to texting while they were driving, though virtually all of them acknowledge knowing it's dangerous! If your child is of driving age, you need to impress upon them the potentially fatal consequences of driving and texting – and of being in a car driven by another teen who is using their smartphone while driving.

b) Data usage

Data management. Familiarize yourself with the data management software available on your child's smartphone. Some phones have built in applications to automatically shut off data when a specified limit is reached, while others data while need to be manually turned on and off. Make sure you and your child know when to turn your data off, and when it makes sense to turn it back on.

With TELUS My Account App parents can learn how to keep up-to-date with how much data is being used for accounts under their name.

c) Social media and applications

Your child will be able to access all kinds of social media applications (e.g., YouTube, Twitter, Instagram, etc.) along with games and other apps via their smartphone. It is really important to understand the permission and privacy settings on social networking accounts they sign up to and apps that you download, which need to be set to where you want them to be. We all need to pay attention to the privacy and permission terms and settings – just don't accept them blindly.

Permission settings control what can and cannot be accessed and shared about you (e.g. contact lists, computer files including photos, and your profile) by a social networking site or mobile app that you subscribe to.

Privacy settings control who can and cannot see your profile and private posts.

Keep an eye on the permissions settings. Every time your child downloads a smartphone app or signs up for a social networking site, they could be allowing its developers to see their personal information which could include their address book, their Facebook or Twitter account information, their location, and even their photos.

Work with your child to keep an eye on their privacy settings. Make sure you know what information is being shared publicly—and what information can be accessed by applications. You child may be sharing more than you intended.

Keep an eye on your privacy settings. Make sure you know what information is being shared publicly—and what information can be accessed by applications that are downloaded onto your child's smartphone.

Safe versus unsafe apps. Every smartphone has a built in apps marketplace which is usually a pretty safe place to get apps. While you will want to make sure you know which social media platforms your child uses, and check the privacy settings the apps ask from your phone, these apps are generally free of viruses and malware. However, many smartphones allow you to download apps from outside the built in app marketplace and this is not recommended.

Many free apps stream advertisements to the device using a small amount of data. They can also be misleading, alerting of virus threats and suggesting installing other software—which could be a paid app or even malicious—to fix the issue.

d) Other important considerations

Google search filters. If your child's phone uses a Google app, it is a good idea to open it and enter into Google settings. Under Search & Now > Accounts & Privacy is a setting called SafeSearch Filter which blocks most explicit content from showing up in Google search results. Make sure that this is turned on to reduce the chance that your child will accidently come across content you would not want them to see.

Cloud services. Today's smartphones support many different cloud services. These are used to back up many different types of content, ranging from contacts and calendars to pictures and videos. Make sure you and your child decide which clouds, if any, to use. Also make sure you check the device to make sure no other cloud services are enabled that you don't know about. Strong passwords are the most important when it comes to cloud services, as these can hold some personal information that you don't want strangers or classmates being able to access.

House rules. With your child create an agreement about the use of their smartphone and family internet use in general. Once you have completed the agreement get all family members to sign it and review it at least every six months. Refer to the next section, Family online rules, for some great examples of family rules and sample agreements.

4. Family online rules

MediaSmarts' research has shown that kids with household rules about Internet use (including smartphones) are less likely to do things like post their contact information, visit gambling sites, seek out online pornography and talk to strangers online. Having a family agreement or set of rules for using the Internet is also a great way for parents and kids to work together on how to be safe, wise and responsible online.

- With younger children, it makes sense for you to set the rules and explain them. As kids get older and explore more of the online world, you can discuss new rules together.
- The most important rule is that if anything ever happens online that makes your children scared, worried or uncomfortable, they should come to you or to another adult they trust. Make sure they know that you're on their side: a lot of kids are reluctant to tell their parents when things go wrong because they're afraid of losing their Internet access or their digital devices.
- For more specific rules, here are some ideas to help you get started:
  - I will always get my parents' permission before giving out any personal information online. This includes my name, gender, telephone number, home or email address, location of my school, my parents' work addresses, email addresses or telephone numbers, their credit card number information and pictures of me or my family.
  - I will not visit any websites that I think my parents would not approve of.
  - I won't share my passwords with anyone (except my parents or a trusted adult) – not even my best friend.
  - I will NOT arrange to meet a friend I have made on the Internet unless a parent or an adult that I trust goes with me.
  - I will ask an adult first before downloading anything, opening attachments or following any links that I don't know are safe.
  - I will always remember that there are other people on the other side of the screen whose feelings can be hurt by what I say and do.
  - I will not be mean or cruel to anyone online, even if someone else is mean to me first.
  - If someone is ever mean to me online, I will remember that it's not my fault.
  - If I see someone else being mean or cruel to someone online, I will do what I can to help the person who is being targeted.
  - If I ever get mad while I'm online, I will let myself cool down before I say or do anything.
  - I will not share anything online that belongs to someone else without their permission.
  - I will always think about how other people might feel before I share something online. I will never share anything that might embarrass someone or hurt their feelings.
  - I will give other people credit when I use their ideas or copy parts of their documents from the Internet in my homework or other projects.
  - I will not disable any filtering software my parents have put on the computer or smartphone.
  - I will not buy things online unless I have my parents' permission.
  - I will never use my phone while behind a wheel driving.

Refer to http://mediatechparenting.net/contracts-and-agreements for some more great examples of contracts you can create with your family.

5. Cyber ethics

Just as protecting youth from the dangers on the Internet is important, so is protecting the Internet from young people who might abuse it. As parents, caregivers, teachers, and adults, we all work to teach youth Internet safety by telling them to keep their personal information safe and avoid predators, but it's just as important to teach youth cyber ethics and show them how their actions can affect others.

- **Share with care.** Youth should know that once something is posted online, they no longer have control over it – even if it's done anonymously. Anything posted can be forwarded, copied, and saved for possibly forever. What may seem funny or "cool" now—like pictures taken at a party, for example—could cause your child a great deal of problems and embarrassment later on. You should talk to your child about the importance of managing how they present themselves online, keeping in mind that employers often review a candidate's online presence and what they find could impact your child's future job opportunities.
- **Protect feelings & reputations.** Not only is your child responsible for maintaining their own reputation online, they also have the power to influence those of others. Cyberbullying happens when a child or teen is embarrassed, humiliated, tormented or harassed by others online. Because it takes place behind screens, youth often forget that cyberbullying has serious, real-life repercussions on all involved. Your child should be aware that even just by 'liking' or sharing an offensive post—acts which are oftentimes perceived as harmless—they help spread the humiliation and thus become part of the problem. Their actions could even constitute a criminal offence.
- **Know the law.** Teens frequently share explicit content with each other through messaging services (commonly known as sexting); however, they may not be familiar with the risks and consequences of sharing such content with others. Cyberbullying legislation in Canada has made the non-consensual distribution of intimate images illegal. The GetCyberSafe.ca website has more information on these laws that your teen should know about.
- **Download cautiously & respectfully.** Another important part of being a courteous and thoughtful cybercitizen is respecting copyright laws. Youth frequently download movies, TV shows, music and software that are copyright protected, which exposes their devices to viruses and could result in legal action taken against them. In addition to discussing these consequences with your child, set the example for them by always obtaining such content legally: a few extra dollars today could save you major headaches down the road.
- **Consider your values.** It's a good idea for parents to communicate your values and mentor your child to be a good cyber citizen. Technology doesn't change the fact that we have to make ethical decisions every day. The same applies with smartphones and social networking - only share information that you're comfortable with others' seeing, don't share passwords, consider appropriate behaviour. Values and ethics is about how your actions affect others. Don't lose sight of what you value and your kids will follow suit.

While enabling parental control features and granting limited permissions on your child's accounts is always a good idea, one of the best ways to help your child be a safe and ethical cyber citizen is by keeping the lines of communication open and setting ground rules for their online activity.

For more information on cybersecurity, visit GetCyberSafe.ca

6. Considerations for keeping your kids safer when using a smartphone

Losing your smartphone

There are great apps likely loaded onto your and your child's smartphone like Apple Find My iPhone or Android Where's My Droid that use GPS to locate your phone in case it goes missing. If you use the app and cannot find your phone please do not try and track it down via the GPS locator – it could put you in a harmful situation. Instead do the following:

- **Know your smartphone's serial number:** When you purchase a smartphone for your child or give them your old phone, copy the International Mobile Equipment Identification number (IMEI), the phone's electronic serial number, and keep it is a safe place. If your phone is lost or stolen you will need this number to report it missing to your service provider and police. To find you IMEI dial *#06# and the number will appear on your phone's screen, or you can find the IMEI number printed on a white label on the battery.
- **Strong passwords:** Before handing over a phone to your child ensure that your set a strong password and you both know what the password is. Also have an agreement that your child will let you know whenever they change the password.
- **Contact your service provider:** The first thing you want to do if the phone is lost or stolen is contact your wireless service provider. They will help you deactivate your device and complete a manufacturers' wipe of all of the information on the phone. Your service provider will also place your phone on a national blacklist, preventing it from working on any Canadian wireless networks.
- **Report your phone as stolen:** Contact your local law enforcement about your phone and give them the phone's IMEI.

"What is your phone's IMEI?"

7. Additional resources

- For an ongoing resource on how to keep you and your family safe on line, please visit TELUS WISE (Wise Internet and Smartphone Education).
- Book a free 1 hour session with a TELUS Learning Centre Specialist for you and your child to learn all of the safety features and functionality of your smartphone.
- The are a number of additional TELUS WISE guides that you may find of value, including:
  - TELUS WISE distracted driving guide
  - TELUS WISE helping our kids navigate their wired world
  - TELUS WISE privacy matters

How you can participate in TELUS WISE

- Visit us at **telus.com/wise** if you have any questions or if you want to book a free in-person TELUS WISE session for you child's school and/or parent group.
- Contact us at **wise@telus.com**
- Join the conversation online with **@TELUS** on Twitter and using **#TELUSWISE**

TELUS