

Helping our kids use their smartphones safely.

A TELUS Wise parent's guide.





# Smartphones have revolutionized the way we live our lives.

For all their benefits, though, they can raise concerns for parents. Questions that come to mind include:

- What are kids doing with their devices?
- Who are they connecting with?
- What apps are they using?
- What content are they accessing?
- How much time are they spending on their device?

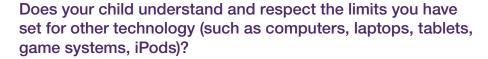
This guide offers practical advice and guidance you can use to help ensure your child has a safe and positive experience with their device.



### Making the decision to give your child a smartphone

Many parents choose to give their kids smartphones as a way of keeping touch with them, or because they don't have a home phone, while for kids, mobile devices are a way to stay connected with friends and family, listen to music, take and share pictures, play games and much more.

When is the right time to give your child a phone? Although this is a frequently asked question, unfortunately, there isn't one "right age" at which to do so. Instead, you need to think about your child's maturity and ability to use a smartphone responsibly. If you're considering getting a smartphone for your child, ask yourself these questions first:



Compared to a desktop, laptop, or even a tablet, it's a lot harder to supervise kids' Internet use when they're using smartphones. Some parents turn to monitoring or parental control software ("spy" or "nanny" apps), however if the only way you can feel safe giving your child a smartphone is by spying on them, they're probably not old enough to have one. While such solutions can provide increased visibility and control, there are possible drawbacks worth considering:

- They can send a bad message about privacy
- They may push kids to use the Internet in unsupervised places, or on unsupervised devices
- Kids may be less likely to come to you if something goes wrong.

Additionally, parental control solutions can provide a false sense of security – they are not always fool proof or perfect, and should not take the place of regular and on-going conversations with your child about smartphone and Internet safety and security. That said, if you do decide to use monitoring software, be open about it: tell your child why you think it's important (for instance, if they have made some bad decisions in the past), and how they can earn your trust.

It is also easier to introduce monitoring software when kids are younger and more receptive to the idea of you monitoring their activities and phone use.



What generally works better is setting household rules about how you expect your kids to behave when using digital devices. If you already have rules, make sure your kids understand that they apply to smartphones as well. If you don't, this is a good chance to talk about them.

See the "Family Online Rules" section in this guide for more information.

# Are you confident your kids will come to you if they run into problems online?

Smartphones mean independence for a lot of kids, but that doesn't mean they are old enough to navigate the digital world, including smartphone ownership and use without you. In fact, this is when it's most important for them to know that it's okay to come to you for help if anything goes wrong – and that you won't 'freak out' if they do.

It's also good to help them prepare for problems before they happen. Make sure you've talked to your child about:

- Cyberbullying: Do they know what to do if someone is mean to them online, or if they see someone else being cyberbullied?
   What should they do if a friend asks them to join in on being mean online to someone else? See the <u>Helping our Kids Deal With</u> <u>Cyberbullying</u> guide for how to talk about this.
- Sexting: Do they understand the potential risks involved, and also why it's wrong to share an intimate image of someone without their permission? (See the tip sheet <u>Talking to Your Kids About Sexting</u> for advice on this topic.)

- FOMO and the Greener Grass Illusion:
- Using social networks on smartphones means being constantly exposed to what others are doing, as well as to photos and posts that have been carefully selected to portray the best of life. Many teens say that FOMO (fear of missing out) is one of the reasons why getting off their phones makes them so anxious, and that comparing their lives to friends' picture-perfect lives on social media can negatively affect their confidence and anxiety. Help them remember that what they're seeing in their friends' feeds is carefully selected (and sometimes edited) to look perfect.
- Privacy and security: Do they understand the privacy tools on their social networks and their phones? Do they know how to set a strong password? Do they know how to turn Bluetooth and GPS off? Do they know how to limit the personal data they share with the apps they use?



### Do you think your kids will be able to turn it off and put it away when they need to?

One of the biggest sources of family conflict around phones has to do with time – how much of it kids spend on their phones, and what they should be doing instead.

There are some times and places when they (and you) should put the phones away:

- At the dinner table: How many times a day are you all in the same room? Make sure your kids understand that family time is for talking to each other, not checking phones.
- In the bedroom: Screens of any kind should not be in bedrooms. The light they emit makes it harder to get to sleep and makes sleep less restful. Phones in the bedroom also can result in the temptation to check them before bed or even during the night. If they (or you) need an alarm clock, buy a real one.
- In the bathroom: This one speaks for itself! Bacteria sticks to phones, and they're harder to wash than your hands. Plus, camera functionality provides another reason to keep them out of the bathrooms (and changing/locker rooms).

- While driving: Not only is it irresponsible and dangerous, distracted driving is against the law in every province and territory except Nunavut. Several provinces also prohibit drivers who don't have their full license from using any screen devices or cell phones while driving, even hands-free, and that's a good rule for all of us to follow.
- While doing homework: Your phone doesn't have to be on for it to distract you. Studies have shown that if it's even within reach, you

use some of your mental energy trying to resist looking at it. When there's work to be done, the phone should be somewhere else.

At other times, you should encourage your kids to use their phones mindfully – only turning them on for a specific reason, instead of checking them out of habit or because they're bored.

A good step towards this is to have them turn off push notifications (those little beeps and buzzes that tell you when you get a text or when someone likes your latest Instagram photo).



# Do you feel they will heed your guidance on which apps they can use and/or only use apps that are age appropriate?

The main reason most kids want a smartphone is so that they can connect to social networks like Snapchat or Instagram, so when you make the decision to give them a smartphone, part of what you're deciding is whether to let your kids use such apps. Most social networks require users to be at least 13 to have an account, so if you let them join earlier, you're violating the terms of service. This may be a problem if you ever have to make a complaint – and if they lie about their age, they may not get protections that are in place for users under 18.

There are some specific types of apps that aren't recommended for children of any age:

- Anonymous messaging or feedback apps: Cyberbullying is common in apps where users don't have any permanent identity. Apps that allow you to use a permanent fake name can be particularly risky, and apps that encourage people to share anonymous feedback with others can also be problematic.
- Location-based apps: Some social networks connect you with other people based on where you are. This not only encourages connecting with strangers, but also meeting them in person.
- **Dating apps:** Kids and teens aren't ready for the content or the interactions that happen on dating apps, not even "friend finder" apps aimed at them. It's also naïve to trust that everyone is who they say they are on such apps.



It's a good idea to set up your child's phone to use your Google Play or App Store account, so that you can set parental content limits, know which apps your kids have downloaded and/or provide approval before new apps can be downloaded.

Just make sure you turn off in-app purchases, so you don't get any surprise charges: here's how to do it for **Apple** and **Android** phones.

# Do you feel like you model good habits with your own phone use?

Remember that what we do speaks twice as loudly as what we say. Before you decide to give your child a smartphone, pay attention to your own phone use for a week or so. Is it sending your kids the messages you want them to receive?

If the answer to all these questions is "yes", then your child may be ready for a smartphone, but it doesn't stop there: you need to keep the conversation going about safe and appropriate online behaviour with your child, whether they're using a smartphone, tablet, computer, networked game console, iPod, or even a smart TV.

Help them understand that technology and smartphone ownership is a privilege, not a right, and that ownership comes with responsibility.

### Once you have decided to give your child a smartphone

### Before purchasing a smartphone, consider these factors:

- 1. Functionality. If you mostly want to give your child a phone for safety or practical reasons, consider getting them a simple phone and plan that only allows them to send texts and make calls. Keep in mind that most smartphones can connect to the Internet via Wi-Fi, so even without a data plan, your child could go online while at places with free Wi-Fi like coffee shops, malls and libraries.
- 2. A test run. You can also start with a "probationary" period. After going through your rules and expectations, tell your child that you're going to let them use a smartphone for a limited amount of time. At the end of that period, review your child's behaviour with them and discuss whether to take away the phone, extend the probationary period or let them have the phone permanently.

You may also want to consider letting them use an old phone you no longer use during the probation period, and purchasing a new phone only after they 'pass' their probation. If you pass down an old phone, remove any apps you don't want your child to use and do a complete wipe of all your data before handing it over.

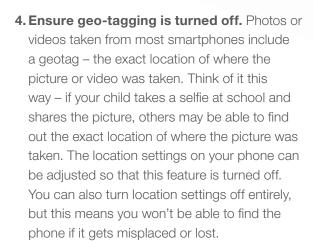


# Before your child starts using their smartphone

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.

- 1. Set up the 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, as "friends" can pick up each other's phones and, as a "joke" make posts on their social media accounts (which kids often leave logged in), or send troublesome texts or emails pretending to be the owner of the phone.
- 2. Install and/or activate remote locate/
  lock/wipe software. Free software lets you lock, track or remotely erase the information on the phone if it is lost or stolen. Both of the major types of phones have built-in services that allow you to find them if they're missing: for iPhones, it's called Find My iPhone, and for Android phones, it's Find My Device.
- 3. Make note of the smartphone's serial number.

Copy the International Mobile Equipment Identification number (IMEI) – the phone's electronic serial number – and keep it in a safe place. If the 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.



- 5. Set up device and content restrictions.
  - You can do this with built-in and/or free features and solutions, such as iOS Screen Time feature or Google Family Link. Please note that filters are not always perfect, with explicit, graphic, or other content deemed inappropriate still accidentally coming through, on occasion.
- 6. Talk about emergency calls. Make sure your child is aware that they can and should call you and/or dial 9-1-1 in an emergency. Add family and emergency contacts to the contact list as well as parents, grandparents, sitters and trusted neighbours. Having a few contacts labeled "In Case of Emergency" lets your child know who they can call if they need help and can't reach you.

#### Additional considerations:

1. Data management. Familiarize yourself with the data management tools available on your child's phone or through your provider. Some phones have built in applications to automatically shut off data when a specified limit is reached; make sure both you and your child know when to turn data off, and when it makes sense to turn it back on.

If you plan on sharing your data plan with your child's device ensure you put a limit on how much data they can consume – thereby preserving data for your own use, and mitigating any overage charges.

- 2. Cloud storage. These services are increasingly common and can help owners retrieve valuable information and files in the event that a device is lost or stolen. Backup solutions that come with your device (such as iCloud or Google Backup) can be safe and cost effective options, but be sure to use a strong password for your accounts. You can also limit backups to happen only over Wi-Fi so as to use less data.
- 3. Social media and applications. Your child will be able to access various social media applications (e.g., Snapchat, Twitter, Instagram, etc.) along with games and other apps on their smartphone. It is really important to understand the permission and privacy settings for these accounts and apps. 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 social media account information, their location, and even their photos.

Encourage your child to pay attention to privacy and permission terms and settings – or at least review them with you. It's best to not accept them blindly, taking the time to review and adjust them to where you want them to be.

- 4. Safe versus unsafe apps. Getting apps only from your phone's official app marketplace (Apple's App Store or Google Play) is the best way to protect phones from malware and viruses. However, it's still a good idea to check app reviews before downloading new apps.
- **5. Notifications.** Many apps are set by default to deliver notifications (usually a visual reminder on your device screen and/or an alert sound) which can make it harder for children to put their phones away. Turning off notifications from everything except voice calls can be useful for helping your children use their devices more mindfully.

6. Passwords. Set a strong password on any social networking accounts or apps that your child uses. Good passwords can help minimize the risk of accounts and apps getting hacked into. They are at least eight characters long and should not be a name or a word found in the dictionary, since these are easily guessed by password-cracking programs.
Make passwords stronger by using an entire phrase, or even the first letters of a phrase, instead of a word — ICARMLP for "I can always remember my laptop password", for instance.

You can also set up two-factor authentication on all of your child's email or social network accounts. This added layer of security will requires your child to enter a code texted to their phone (or your phone) each time they login, or only when they need to recover a lost password.

Change some of the letters into numbers and

add special characters, too.

### If your child loses their smartphone

If your child's smartphone is lost and you're not able to find it using Find My Phone or Find My iPhone, contact your wireless service provider. They will help you deactivate the device and possibly even place it on a national blacklist, preventing it from working on any Canadian wireless networks.

If you know for certain that the phone was stolen, contact your local law enforcement and give them the phone's IMEI number.

### 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.

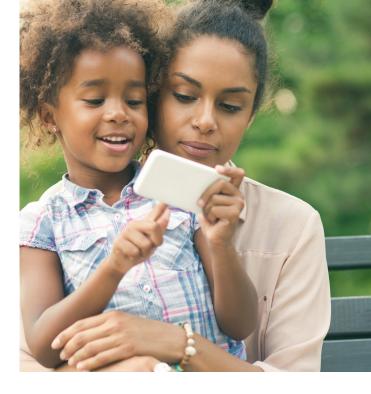
With younger children, it makes sense for you to set the rules and explain them. As kids get older and explore more of the online world, you can discuss new rules together.

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 another adult they trust. Make sure they know that you're on their side and will not over react; 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 follow all of my school's rules about using phones.
- I will not use my phone when I am driving, walking, cycling or doing anything else that requires focus.

- I will not visit any websites or use any apps that I think my parents would not approve of.
- I will not install any new apps or buy anything online without my parents' permission.
- I will not be mean or cruel to anyone online, even if someone else is mean to me first.
- 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.
- 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, and talk to a trusted adult about it.
- If I ever get mad while I'm online, I will let myself cool down before I say or do anything.
- I will get my parents' permission before sharing any personal information online. This includes my name, gender, telephone number, home or email address, school name, parents' work addresses, email addresses or telephone numbers, their credit card information and pictures of me or my family.
- I won't share my passwords with anyone (except my parents or a trusted adult) – not even my best friend – and if I change my passwords, I will let my parents know.
- I will not arrange to meet a friend I have made on the Internet unless I have talked to my parents about it and a parent goes with me.



- I will ask a trusted adult first before downloading anything, opening attachments or following any links that I don't know are safe.
- I will not share anything online that belongs to someone else (including pictures of others) without their permission.
- I will give other people credit if I use their ideas or content for school projects or other purposes.

You can also download the **TELUS Wise smartphone contract** to establish ground rules that you and your children will follow online.



Find more resources on keeping your family safe in our digital world, visit the **MediaSmarts** or **TELUS Wise** websites.

# How you can participate in TELUS Wise.

- Visit <u>telus.com/wise</u> to learn more, or book a free in-person TELUS Wise workshop for your child's school and/or parent group.
- Take the TELUS Wise Digital Pledge at telus.com/digitalpledge.
- Contact us at wise@telus.com.
- Join the conversation online with @TELUS on Twitter and using #TELUSWise.

