



Teacher Unit Plan

Junior Grades

Cybersecurity Resources for Teachers & Educators

About the resources

These resources are a free, comprehensive set of teaching materials; created by cybersecurity experts and Canadian educators, and linking directly to the Ontario curriculum. Available in four grade groupings, the language, learning goals and activities have been adapted to learners in primary (grades 1 to 3), junior (grades 4 to 6), intermediate/senior (grades 7 and 8) and high school (grades 9 to 12).

Resources include start-to-finish teaching materials, such as unit plans and recommended rubrics for teachers, and corresponding lesson worksheets for students. Lessons cover various essential topics related to digital citizenship, cybersecurity and cyber safety – such as cyber respect and online kindness (cyberbullying), communicating safely online, positive digital footprint and more!

Using the resources

The goal of these resources is to provide a modern, curriculum-linked set of materials for Ontario educators and teachers, empowering and preparing them to equip youth with the knowledge and tools they need to use technology in a positive way, while at the same time being able to identify and prevent the associated risks.

These resources are accessible and can be easily implemented in the physical classroom or the online, virtual classroom environment.

The Catalyst has proactively offered two versions of all resources:

1. **A PDF version**, intended to be a downloadable, ready-to-use resource for educators and teachers. Download, print and share physical or digital copies with students for instant use.
2. **A Microsoft Word version** contains the same content as the PDF version. However, the Word version is editable, and allows for language and worksheets to be modified by educators and teachers as needed. It is recommended to edit the unit plans and lessons to accommodate the various learning needs and abilities of your students, or to incorporate additional or preferred modalities into the lessons.

Additional cybersecurity resources

Cybersecurity, cyber safety and digital citizenship are relatively new areas of study; and, although these resources have been developed with the potential of limited technical or cyber experience in mind, we recognize that additional information may be needed to supplement an understanding of the topics covered.

We encourage educators and teachers to conduct independent research, and take advantage of the multitude of free resources available online, including the Rogers Cybersecure Catalyst youth resources:

<https://www.cybersecurecatalyst.ca/cybersecurity-for-k-12>

About the organization



The Rogers Cybersecure Catalyst, ‘the Catalyst’, is a not-for-profit corporation owned and operated by Ryerson University. The Catalyst strives to empower Canadian citizens and businesses to take full advantage of the

opportunities in the virtual space, and tackle the serious challenges of cybersecurity, through training and certification; commercial acceleration and support for cyber scale-ups; applied research and development; and public education.

About the initiative



In 2019, the Rogers Cybersecure Catalyst partnered with Rogers Communications Inc., to help develop the Canadian cybersecurity ecosystem and fuel Canada’s digital economy. As a leading technology and media company in Canada, Rogers is committed to keeping Canadians cyber safe.

Together, the Catalyst and Rogers have identified a need to foster stronger collaboration between the cybersecurity community, academia and educational partners, to build awareness and understanding in cybersecurity, especially for youth.



Ontario Language Curriculum Overall Expectations

Oral Communication	Writing	Media Literacy	Health & Physical Education
<p>1. Listening to Understand: Listen in order to understand and respond appropriately in a variety of situations for a variety of purposes;</p> <p>2. Speaking to Communicate: Use speaking skills and strategies appropriately to communicate with different audiences for a variety of purposes;</p> <p>3. Reflecting on Skills and Strategies: Reflect on and identify their strengths as listeners and speakers, areas for improvement, and the strategies they found most helpful in oral communication situations.</p>	<p>1. Developing and Organizing Content: Generate, gather, and organize ideas and information to write for an intended purpose and audience;</p> <p>2. Using Knowledge of Form and Style: Draft and revise their writing, using a variety of literary, informational, and graphic forms and stylistic elements appropriate for the purpose and audience;</p> <p>3. Applying Knowledge of Conventions: Use editing, proofreading and publishing skills and strategies, and knowledge of language conventions, to correct errors, refine expression and present their work effectively;</p> <p>4. Reflecting on Skills and Strategies: Reflect on and identify their strengths as writers, areas for improvement, and the strategies they found most helpful at different stages in the writing process.</p>	<p>1. Understanding Media Texts: Demonstrate an understanding of a variety of media texts;</p> <p>2. Understanding Media Forms, Conventions and Techniques: Identify some media forms, and explain how the conventions and techniques associated with them are used to create meaning;</p> <p>3. Creating Media Texts: Create a variety of media texts for different purposes and audiences, using appropriate forms, conventions and techniques;</p> <p>4. Reflecting on Skills and Strategies: Reflect on and identify their strengths as media interpreters and creators, areas for improvement, and the strategies they found most helpful in understanding and creating media texts.</p>	<p>1. Social-Emotional Learning Skills: Apply, to the best of their ability, a range of social-emotional learning skills as they acquire knowledge and skills in connection with the expectations in the Active Living, Movement Competence and Healthy Living strands for this grade;</p> <p>2. Healthy Living: Demonstrate the ability to make connections that relate to health and well-being – how their choices and behaviours affect both themselves and others; and how factors in the world around them affect their own and others' health and well-being.</p>

Culminating Task: Digital Citizenship Infographic

Category	Level 4	Level 3	Level 2	Level 1
Knowledge	Demonstrates thorough knowledge of chosen theme in cybersecurity Uses 5+ sources of information	Demonstrates considerable knowledge of chosen theme in cybersecurity Uses 3-4 sources of information	Demonstrates some knowledge of chosen theme in cybersecurity Uses limited sources of information	Demonstrates limited knowledge of chosen theme in cybersecurity Limited evidence of research
Thinking	Uses graphic design skills, such as vivid graphics, with a high degree of effectiveness	Uses graphic design skills, such as vivid graphics, with a considerable degree of effectiveness	Uses graphic design skills, such as vivid graphics, with some degree of effectiveness	Uses graphic design skills, such as vivid graphics, with limited effectiveness
Communication for different audiences and purposes	Communicates intended message to audience with a high degree of effectiveness Clear main idea and thought-provoking supporting details	Communicates intended message to audience effectively Clear main idea and adequate supporting details	Communicates intended message to audience with some degree of effectiveness Main idea is lacking clear support	Communicates intended message to audience with limited effectiveness Main idea is unclear
Application of knowledge and skills	Transfers knowledge and research skills to new contexts (Infographic) with a high degree of effectiveness	Transfers knowledge and research skills to new contexts (Infographic) effectively	Transfers knowledge and research skills to new contexts (Infographic) somewhat effectively	Transfers knowledge and research skills to new contexts (Infographic) with limited effectiveness

Teacher Feedback:

Final Grade:

Unit Overview

This unit is designed to teach young students about how to be stewards of digital citizenship in their classroom communities and in the digital community beyond the classroom. Digital citizenship refers to the responsible and safe use of technology and the Internet by anyone who uses it to engage with society.

This unit has assessments throughout and leads to a culminating task: a student-developed Infographic (an advertisement or a visual representation of information) on one of the six topics taught in this unit, or beyond, depending on whether you'd like to make this an inquiry-based task.

Lessons Overview

Lesson 1: Cyber Respect & Online Kindness

Lesson 2: Positive Digital Footprint

Lesson 3: Safe Communication Online

Lesson 4: Passwords & Passcodes

Lesson 5: The Truth Online

Lesson 6: Digital Citizenship Infographic

Teacher Resource: Infographic Rubric

For additional information on the topics covered or additional supporting materials, check out the Rogers Cybersecure Catalyst downloadable Youth Resources:

<https://www.ryerson.ca/cybersecure-catalyst/youth/resources/>

Lesson 1: Cyber Respect & Online Kindness

Lesson Plan for Parent(s)/Guardian(s)

Digital literacy is a fundamental component of the 21st century, and vital for civic and social participation, accessing public services, and succeeding in a digitizing economy (as explained via a Brookfield Institute [recent publication](#)). As such, in this unit, students will be learning about digital citizenship and how to manage their evolving digital presence.

Today, students will be taking a close look at how to communicate and exist online respectfully. They'll be learning about how to recognize and respond to negative interactions online (cyberbullying), and how to put their best "digital foot" forward.

Hook

10 minutes

Greet students as they enter the classroom
Great time to check in about well-being

Cyber Respect & Online Kindness KWL
(Know, Want and Learned chart)

Assess what the students already know about cyberbullying, what it means to show cyber respect and online kindness, and where their curiosities naturally lie, by completing the KWL Chart in the correlating Lesson 1 handout.

Suggestion: Share a definition of cyberbullying and online kindness as a guide for class discussion when reviewing what students wrote or drew on their handouts.

Sample definitions:

Cyberbullying: When someone (or a group) is being mean to someone else through the Internet or by using technology (like a cellphone or a tablet). It can include things like name-calling, spreading rumours, forcing someone to do something they don't want to do, or making fun of someone and getting others to join in.

Suggested examples:

- Posting mean things (words, emojis or pictures) online, to or about another person, to hurt their feelings.
- Using another person's online profiles to post embarrassing things about them.
- Posting embarrassing photos or videos of a person.
- Messages posted online or texted to someone that hurt someone's feelings.

Online kindness: Using the Internet in a positive way, such as writing nice messages on social media or sharing photos/videos online to brighten someone's day.

Suggested examples:

- Always treat others the way we want to be treated.

	<ul style="list-style-type: none">• Treat others with kindness at all times – it’s always easier to be kind than to be mean.• When seeing someone being kind to someone else, give them a compliment and help them feel good about being kind. <p>What do you know already and what do you want to learn? We’ll fill out what we’ve learned as we go.</p> <p>Cyber Respect & Online Kindness</p> <table><tr><th>What do I Know?</th><th>What do I Want to Know?</th><th>What have I Learned?</th></tr><tr><td></td><td></td><td></td></tr></table>	What do I K now?	What do I W ant to Know?	What have I L earned?			
What do I K now?	What do I W ant to Know?	What have I L earned?					
<p>Learning Goals & Success Criteria</p> <p>5 minutes</p>	<p>Share learning goals for purposeful learning. Success Criteria let students know what they’ll be able to do when they’ve learned this.</p> <p>Learning goals:</p> <ul style="list-style-type: none"><input type="checkbox"/> I can recognize Cyber Respect & Online Kindness<input type="checkbox"/> I know how to respond to negative interactions online<input type="checkbox"/> I can recognize bullying online (cyberbullying)<input type="checkbox"/> I am an Upstander						
<p>Input & Modelling</p>	<p><i>Teach and show the content and skills students need to know to be successful. Model with examples that clarify understanding.</i></p> <ul style="list-style-type: none">• Cyber Respect Looks Like, Feels Like, Does not Feel Like• Online Kindness Looks Like, Feels Like, Does not Feel Like <p>Students can brainstorm examples of online kindness by filling out the chart independently, in groups, and then as a class.</p> <p>By allowing students to share experiences that are relevant to them, you’ll get a sense of their online space. For example, if many students are giving examples from online games, you can tailor the information you share toward gaming.</p>						
<p>Guided & Independent Practice</p> <p>20 minutes</p>	<p>Observe, prompt, support, enrich</p> <p>Review what an Upstander is and how they’re different from Bystanders.</p>						

	<p>Sample Definitions</p> <ul style="list-style-type: none"> • Upstander: Someone who speaks up for and/or acts in support of someone in need. • Bystander: Someone who knows about or sees something hurtful happening, but chooses to not get involved. <p>In small groups, have students discuss why someone may not feel comfortable being an Upstander. Potential answers may include:</p> <ul style="list-style-type: none"> • <i>Maybe the Bystander was once bullied, and doesn't want to risk being bullied again.</i> • <i>Maybe the Bystander doesn't know what to say.</i> • <i>Maybe the Bystander doesn't think it's their responsibility to stand up.</i> <p>It's not always the easy or simple choice to stand up for what's right, but it's still important to do so.</p> <p>Discuss: Although being an Upstander may feel uncomfortable, it's a great option in defence of cyberbullying.</p> <p>Optional Extension: Provide and discuss examples of <i>how</i> someone can be an Upstander. Suggested examples include:</p> <ul style="list-style-type: none"> • If the bully is someone they know, kids can help the bully see kindness by being kind to them, like posting something positive about them or inviting them to join an online community. • Kids can get together with friends, classmates or teammates who also want to be Upstanders – a group of positive people looking out for each other can make a big difference for someone who's been hurt by a bully! <p>Important notes:</p> <ul style="list-style-type: none"> • Remind students that they shouldn't confront a bully who is a stranger, either in person or online. Instead, they should tell a parent/guardian, teacher or other trusted adult. • Remind students that they can always connect with Kids Help Phone by texting: 686868 or calling: 1-800-668-6868 from across Canada, 24 hours a day, 7 days a week.
<p>Check for Understanding</p> <p>10 minutes</p>	<p>Observations, Formative Assessment</p> <p>Response on Lesson 1 handout:</p>

	<div>Why might a student not feel comfortable being an Upstander?</div>
Closure	<p><i>Review, questions, wrap-up, discussion, appreciations</i></p> <p>A feelings chart for online kindness can serve as a guide or contract for the classroom community moving forward in the digital space.</p> <p>You could create an anchor chart or a contract for all of the students to sign, including the feelings your class came up with.</p>
Resources	
Assessment	<p><i>For Learning:</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> Observation ✓ <input type="checkbox"/> Anecdotal notes <input type="checkbox"/> Checklist <input type="checkbox"/> Conferencing/conversations <input type="checkbox"/> Work samples/products ✓ <input type="checkbox"/> Check-ins ✓ <p><i>As Learning:</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> Rubric <input type="checkbox"/> Success criteria ✓ <input type="checkbox"/> Self-reflection <input type="checkbox"/> Other: Ticket Out the Door <i>Student Response can be Used as a Ticket Out The Door</i> ✓ <p><i>Of Learning:</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> Quiz <input type="checkbox"/> Test <input type="checkbox"/> Presentation <input type="checkbox"/> Assignment <input type="checkbox"/> Other product
Notes:	

Lesson 2: Positive Digital Footprint

Lesson Plan for Parent(s)/Guardian(s)

Students have many reasons to have a positive digital footprint; that is, the impression they leave behind after posting online, messaging in a group chat, and other activities they participate in online. Once something is posted online, it's there to stay, so it's important for students to be very mindful of their actions online.

Students will be learning about how their actions online affect those around them, and how to build thoughtful and positive digital footprints that will represent them appropriately.

Hook

10 minutes

Greet students
Great time to check in about well-being
Engage prior knowledge

The way you conduct yourself online is your digital footprint. It consists of anything you post or like online, and what comes up when your name is searched.

Students have many reasons to have a positive digital footprint, as they represent themselves, their families, their schools and communities.

Suggested discussions include:

What could lead to a *negative* digital footprint?

Examples include:

- Saying mean things about other people through a text message, in a chatroom, etc. (i.e., cyberbullying).
- Sending or sharing inappropriate photographs, videos, images or posts.
- Selecting rude or distasteful screen names or email addresses.

How to create a *positive* digital footprint?

Examples include:

- Being kind and respectful toward others at all times.
- Keeping posts positive (e.g., highlight special skills, achievements, helping other people, etc.).
- Humour is a common and great tool, but kids need to be careful! Advise them to keep humour light and positive by avoiding sensitive topics; and never use humour to get a laugh at someone else's expense.

Introduce the Lesson 2 handout *Ripples of Your Online Actions*, and give some examples of how an individual's actions online have ripple effects.

For example, sharing an accomplishment could make your parents feel proud, but sharing your location could make your

	<p>parents very worried.</p> <p>Optional Extension:</p> <p>Consider reading the picture book <i>Ping</i> by Ani Castillo, and discuss that you can only control what you put out into the world.</p> <p>You may choose to acquire the book ahead of time, or watch a video of Ani Castillo reading her book here: https://www.youtube.com/watch?v=fqTZ3T0_uQ</p> <p>The messages and themes are a great place to start when discussing a positive digital footprint, and good cyber and real-life citizenship.</p>
<p>Learning Goals & Success Criteria</p> <p>5 minutes</p>	<p>Share learning goals for purposeful learning. Success Criteria let students know what they'll be able to do when they've learned this.</p> <p>Learning goals:</p> <ul style="list-style-type: none"> <input type="checkbox"/> I understand that I'm responsible to myself, my friends and family, and my community in creating a positive digital footprint <input type="checkbox"/> I know strategies for building a positive digital footprint and repairing a damaged footprint
<p>Input & Modelling</p>	<p><i>Notes for Accommodations go here (supplementary materials)</i></p> <ul style="list-style-type: none"> • Content • Process • Learning environment • Product <p>Once students have worked on Lesson 2 <i>Ripples of Your Online Actions</i> handout independently, have them add more examples by working with a partner, and have the class share some examples.</p>
<p>Guided & Independent Practice</p> <p>20+ minutes</p>	<p><i>Observe students working together during group work.</i></p> <p>If there's time, ask students to re-read the "How to Create a Positive Digital Footprint" section, and complete the bonus question at the end of the handout.</p> <p>This can be used as an assessment for learning.</p>
<p>Check for Understanding</p> <p>10 minutes</p>	<p>Answer the following question: <i>Can you think of additional ways to build your positive digital footprint?</i></p>

Closure	<p>Share student responses.</p> <p>Express appreciation to the students for sharing openly about an important topic.</p>
Resources	Resources for the Educator
Assessment	<p>For Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Observation ✓ <input type="checkbox"/> Anecdotal notes ✓ <input type="checkbox"/> Checklist <input type="checkbox"/> Conferencing/conversations ✓ <input type="checkbox"/> Work samples/products ✓ <input type="checkbox"/> Check-ins <p>As Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Rubric <input type="checkbox"/> Success criteria <input type="checkbox"/> Self-reflection <input type="checkbox"/> Other <p>Of Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Quiz <input type="checkbox"/> Test <input type="checkbox"/> Presentation <input type="checkbox"/> Assignment <input type="checkbox"/> Other product
Notes:	

Lesson 3: Safe Communication Online

Lesson Plan for Parent(s)/Guardian(s)

There are plenty of benefits to using technology that students and their families are already well aware of. Today, we're informing students about some online safety measures, so they can continue to enjoy the online space with fewer risk factors.

Hook 10 minutes	<p><i>Greet students</i> <i>Great time to check in about well-being</i> <i>Engage prior knowledge, reminder of the last lesson</i></p> <p>In the previous lesson, we discussed our digital footprints and how to create an online presence that represents us in a positive way. Today, we'll be learning about how to be safe online, and become aware of the potential risks when chatting or sharing with others, while still having fun!</p> <p>Thumbs Up/Thumbs Down Activity Have students show the answer "yes" with a Thumbs Up and "no" with a Thumbs Down to gauge their experience being online.</p> <ul style="list-style-type: none"><input type="checkbox"/> I have an account on a gaming website or console (PlayStation, Xbox, etc.)<input type="checkbox"/> I have my own email address or online account<input type="checkbox"/> I have my own social media profile (Snapchat, TikTok, etc.)<input type="checkbox"/> I have my own, or have access to, an electronic device such as a laptop, tablet or cellphone <p>Based on the results in your classroom, lead a discussion about some of the risks associated with these activities and sharing personal information online.</p> <p>Have students share their experiences about when and how they use devices, at home or at school.</p>
Learning Goals & Success Criteria 5 minutes	<p>Share learning goals for purposeful learning. Success Criteria let students know what they'll be able to do when they've learned this.</p> <p>Learning goals:</p> <ul style="list-style-type: none"><input type="checkbox"/> I know strategies to protect myself from online risks<input type="checkbox"/> I can recognize unsafe communication online
Input & Modelling	<p>At this age, time spent online often includes chatting with friends, sharing pictures, playing a game or watching videos. Some of these activities take place using social media platforms, mobile apps or a messaging system that can allow kids to have conversations with people they may have never met in-person or don't know very well. In such cases, it's hard to know who's on the other end of the device, or what their intentions may be. That's why, in order to communicate safely</p>

online, it's important to limit the amount of private information shared publicly, as strangers may try to use this information to create fake friendships in hopes of gaining something personal about the kid and use that information to cause them harm.

When online, students should always be vigilant and on the lookout for "online charmers".

Sample definition:

Charmer: Someone with a fun personality, who may come across as cool and friendly, but usually uses their charm to control others. Online charmers aren't very easy to spot because they often look like they're trying to be genuinely nice. They use private information about a person, or how that person is feeling, as an opportunity to gain trust.

To help kids identify when/if they may be communicating with a potential online charmer while using devices, explain that kids should keep a lookout for, and tell a parent/guardian, teacher or other trusted adult if:

- Someone starts by asking simple questions, but then gets more personal.
- Someone compliments them, claims to like all the same things or offers to buy them things; this is often a trick to gain trust!
- Someone tries to get kids to feel safe enough to meet in person, join a video chat, or send them pictures.

Advice to offer kids when they're communicating with others online:

- Encourage kids to trust their gut! If something or someone feels "creepy" or makes them uncomfortable, even if they don't understand why, they should listen to that feeling. Explain to kids that this feeling often happens when, deep down inside, they know something is wrong.

If a kid thinks they're potentially interacting with a charmer, they should take the following actions*:

- **STOP:** Stop talking to the charmer right away.
- **BLOCK:** Block the charmer, but don't delete the messages; instead, share those with a trusted adult.
- **TALK:** Talk to a parent/guardian, teacher or other trusted adult immediately.

**See infographic in Lesson 3 handout*

	<p>Sample class conversation starters include:</p> <ul style="list-style-type: none"> • What are some ways to recognize an online charmer? • What is considered personal, or private, information? • What actions can you take to stay safe online?
Guided & Independent Practice 20 minutes	<p><i>Observe, prompt, support, enrich</i></p> <p>Provide students with time to create their safe communication online information poster.</p>
Check for Understanding 10 minutes	<p><i>Observations, formative assessment</i></p> <p>Make sure you're available to answer students' questions. Depending on the theme of their poster, they may need some support on how to make their information positive and empowering.</p>
Closure	<p><i>Review, wrap-up, discussion, appreciations</i></p> <p><i>Have you ever had a strange feeling about someone or something when using technology? What made it feel strange? Who did you tell?</i></p> <p>Tip: Try using comparisons from in-person situations to explain a gut feeling – such as when someone is staring for too long or is physically following too closely.</p> <p>Discuss: <i>What is considered personal, or private, information? Why is it dangerous to share this type of information online or with strangers?</i></p>
Resources	Resources for the Educator
Assessment	<p>For Learning:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Observation✓ <input type="checkbox"/> Anecdotal notes <input type="checkbox"/> Checklist <input checked="" type="checkbox"/> Conferencing/conversations✓ <input type="checkbox"/> Work samples/products <input type="checkbox"/> Check-ins <p>As Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Rubric <input type="checkbox"/> Success criteria <input type="checkbox"/> Self-reflection <input type="checkbox"/> Other <p>Of Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Quiz <input type="checkbox"/> Test <input type="checkbox"/> Presentation <input type="checkbox"/> Assignment

	<input type="checkbox"/> Other product
Notes:	

Lesson 4: Passwords & Passcodes

Lesson Plan for Parent(s)/Guardian(s)

What are passcodes? Passcodes (also known as passwords) are like keys for keeping personal and private information safe from others. Passcodes can be a series of random words put together; a memorable phrase; or a combination of words, numbers and symbols unique to the user – like a fingerprint!

Today, students will be learning about strong passwords and how to protect their information online.

Hook 10 minutes	<p><i>Greet students</i> <i>Great time to check in about well-being</i> <i>Engage prior knowledge</i></p> <p>Brainstorm <i>where</i> passwords are used. Brainstorm <i>why</i> we use passwords. Brainstorm the most popular passwords.</p> <p><i>Can be done as a class, in small groups, in partners.</i></p> <p>Sample definition:</p> <p>Passcodes: Think of passcodes (more commonly, “passwords”) like keys to a home. No one can use their keys to enter someone else’s home because keys are unique in shape, length and the number of grooves they have; the household key protects the keyholder, their family and property. Passcodes are keys to keeping personal and private information safe from others online. Passcodes can be a series of random words put together; a memorable phrase; or a combination of words, numbers and symbols unique to the user – like a fingerprint!</p> <p>According to Splash Data, some of the most popular passwords in 2020 were:</p> <ul style="list-style-type: none">• 123456• 123456789• password• 1234567• 12345678• 12345• iloveyou• 11111• 123123• Password1
Learning Goals & Success Criteria	<p>Share learning goals for purposeful learning. Success Criteria let students know what they’ll be able to do when they’ve learned this.</p> <p>Learning goals:</p>

5 minutes	<ul style="list-style-type: none"> <input type="checkbox"/> I can create a strong and secure password <input type="checkbox"/> My passwords are not easy to guess <input type="checkbox"/> I know how to protect my password from others
Input & Modelling	<p>Teach and show the content and skills students need to know to be successful. Model with examples that clarify understanding.</p> <p><i>Notes for Accommodations go here (supplementary materials)</i></p> <ul style="list-style-type: none"> • Content • Process • Learning environment • Product <p>Teach students how to protect their digital footprints and personal information by protecting their passwords. Using the handout as a guide, review how to create a strong password.</p> <p>Creating strong passwords:</p> <ul style="list-style-type: none"> • Longer is stronger! Long passcodes are harder for others to guess. Most online accounts require a minimum passcode length of 10 characters; however, a recommended length is 12-15 characters. • Use a passphrase! A passphrase can be a few random words used together that are easy to remember. If you need help thinking of one, try using a combination of words that rhyme. • Never use any personal or private information in a passcode or passphrase, such as information that someone might already know or easily get from someone else. • Do not use repeating numbers like '777' or use a number count like '123' / '321', or a significant date like a birthdate or phone number. These are too easy to guess! • Create passcodes with a variety of characters! Include uppercase letters (ABC) and lowercase letters (abc), numbers (123) and symbols (!, @, #). Using all four types makes for a super strong passcode! <p>Creating a strong password is very important, but that's only the first step to keep it safe. The second step is to keep it to yourself! Here are just some ways kids can protect themselves and their passwords:</p> <p>Protecting passwords:</p> <ul style="list-style-type: none"> • Always use a unique passcode for each profile because, if a password is stolen from one account, other accounts will still remain protected! • Do not reuse old passcodes – even if the old passcodes were for other accounts or profiles. • Best practice is to change passcodes from time to time because even strong passwords can eventually be guessed. You can set a date on your calendar to remind you to do this. • Don't share passwords with friends, not even best friends! Depending on your rules at home, passwords should be shared with parents/guardians only, for emergency purposes.

	<ul style="list-style-type: none"> • Be aware of physical surroundings! Watch out for others trying to look at your password as you type it into your computer or other devices. • Avoid logging into accounts on other people's devices, as passwords can be easily retrieved. If absolutely necessary, be sure to log out of profiles and devices when finished.
Guided & Independent Practice 20 minutes	<p><i>Observe, prompt, support, enrich</i></p> <p>Task students with creating their own examples of passwords that follow the best practices outlined in the Lesson 4 handout – passwords that would be easy for them to remember, but difficult for anyone else to guess.</p> <p>Important note: Remind students that, based on their rules at home, they may have to share their passwords with their parents/guardians.</p>
Check for Understanding 10 minutes	<p><i>Observations, formative assessment</i></p> <p>Optional Extension: Check the strength of the students' example passwords on Kaspersky Password Check: https://password.kaspersky.com/</p>
Closure	<p><i>Review, wrap-up, discussion, appreciations</i></p> <p>Share example passwords, discuss strength and how examples could be improved, to inspire the class. Remind students that once a password has been written down or shared with their peers, it should not be used as an actual password for one of their online accounts!</p>
Resources	<p>Resources for the Educator</p>
Assessment	<p>For Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Observation ✓ <input type="checkbox"/> Anecdotal notes <input type="checkbox"/> Checklist <input type="checkbox"/> Conferencing/conversations <input type="checkbox"/> Work samples/products <input type="checkbox"/> Check-ins <p>As Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Rubric <input type="checkbox"/> Success criteria <input type="checkbox"/> Self-reflection <input type="checkbox"/> Other: Password checked ✓ <p>Of Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Quiz <input type="checkbox"/> Test <input type="checkbox"/> Presentation

	<input type="checkbox"/> Assignment <input type="checkbox"/> Other product
Notes:	

Lesson 5: The Truth Online

Lesson Plan for Parent(s)/Guardian(s)

The concept of “truth” has never been more unclear than it is today. Before the rise of the Internet, people consumed news from mainstream media outlets that, for the most part, had reputations for credible and honest reporting. Now, people have the ability to easily create and share content, which leads to the increased potential to share fake or misleading content that’s uninformed, or possibly biased, in nature.

In today’s lesson, students will be learning how to critically assess what they see on the Internet and in the media, in order to verify if what they’re consuming is true.

Hook

10 minutes

Greet students

Great time to check in about well-being

Engage prior knowledge, reminder of the last lesson

Before conducting any research online pertaining to the students’ chosen topic for their Digital Citizenship Infographic (Lesson 6 culminating assignment), they’ll be learning about tools for consuming information, and how to detect whether or not the information is true.

Have your students heard the term “*fake news*” before? If not, lead a class discussion and see what they already know about *fake news*; the spread of online lies; and the importance of checking that what you see, hear or read online is in fact, true.

Sample conversation starter:

It’s often hard to pinpoint why people lie online. Often, the goal is to cause some sort of reaction, such as anger or excitement. Sometimes it’s meant to change people’s beliefs about a certain topic, or to make money by selling a product or idea (such as misinformation from advertising companies). Alternatively, sometimes people simply make mistakes – authors, bloggers or journalists may have forgotten to check the facts, or honestly believed they had the correct information.

Types of online lies, and sample explanations for kids:

- **Misinformation:** Online information, usually in the form of articles, videos or social media posts that try to make kids think they’re true or factual pieces of information, but are actually fake and meant to spread lies or cause a reaction.
- **Harmful Internet challenges:** Usually, these challenges encourage kids to do silly or funny things, like dance moves or try a super spicy hot sauce; however, sometimes these challenges can try to scare people or even attempt to get them to hurt themselves.
- **Fake online contests:** Contests can be very tempting, as they often promise some sort of reward, such as money or free items for doing something as simple as answering a question or filling out a form. However, this can be a quick way for

	<p>unknown people or companies to get kids' personal or private information.</p> <p>Discuss examples of where online lies can be found. Suggested responses include: online games, videos, images, news, websites, social media, and more.</p>
Learning Goals & Success Criteria 5 minutes	<p>Share learning goals for purposeful learning. Success Criteria let students know what they'll be able to do when they've learned this.</p> <p>Learning goals:</p> <ul style="list-style-type: none"> <input type="checkbox"/> I can use critical thinking skills to recognize online lies or false information that's presented in the media
Input & Modelling	<p>Teach and show the content and skills students need to know to be successful. Model with examples that clarify understanding.</p> <p><i>Notes for Accommodations go here (supplementary materials)</i></p> <ul style="list-style-type: none"> • Content • Process • Learning environment • Product <p>With the handout as a guide, review the common categories of online lies that kids may come across while browsing the Internet, watching their favourite videos on YouTube, or while playing a game on their tablet.</p> <p>Explain that the Internet is a limitless place that is literally growing larger every day. It's full of information and resources, making the ability to conduct an efficient online search a highly valuable skill.</p> <p>Encourage kids to be an online detective! It can be hard for kids to tell the difference between truth and lies online, so they may ask for help quite a bit! Suggest that kids ask the following questions about what they come across online:</p> <ul style="list-style-type: none"> • Is this too good, or too bad, to be true? • Does it say bad things about people or groups of people? • Is it weird, scary or gross? • Have you heard it before from anywhere else? Have your friends talked about it? Have you learned about it at school? Is this just a rumour? • Can you find it anywhere else online? Have you seen it anywhere offline, like on television or radio?

	Important note: Remind your students that if they come across anything online that they're unsure is real or not, they should show it to a parent/guardian or trusted adult right away.
Guided & Independent Practice 20 minutes	<p><i>Observe, prompt, support, enrich</i></p> <p>Once students have reviewed the handout and key critical thinking questions to ask themselves when coming across information online, ask them to find one article, and decide whether it's credible or fake.</p> <p>The article must be related to one of the themes covered so far:</p> <ol style="list-style-type: none"> 1. Cyber Respect & Online Kindness (Cyberbullying) 2. Positive Digital Footprint 3. Safe Communication Online 4. Passwords & Passcodes 5. The Truth Online <p>Optional Extension: You can provide younger kids with a few tools to help them become online detectives and “decode” what they're reading and watching online, such as kid-friendly search engines. Kiddle.co is a web search engine and online encyclopedia emphasizing safety for young children. Encouraging kids to use Kiddle will help them avoid seeing inappropriate content in their search results; and it's also a good tool to help them verify the information they're coming across elsewhere.</p>
Check for Understanding 10 minutes	<p><i>Observations, formative assessment</i></p> <p>Have students present their article, and their reasons for believing it's credible or fake, in small groups.</p>
Closure	<i>Review, wrap-up, discussion, appreciations</i>
Resources	Resources for the Educator
Assessment	<p>For Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Observation ✓ <input type="checkbox"/> Anecdotal notes <input type="checkbox"/> Checklist <input type="checkbox"/> Conferencing/conversations ✓ <input type="checkbox"/> Work samples/products ✓ <input type="checkbox"/> Check-in <p>As Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Rubric <input type="checkbox"/> Success criteria ✓ <input type="checkbox"/> Self-reflection <input type="checkbox"/> Other

	<p>Of Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Quiz <input type="checkbox"/> Test <input type="checkbox"/> Presentation <input type="checkbox"/> Assignment <input type="checkbox"/> Other product
<p>Notes:</p>	

Lesson 6: Digital Citizenship Infographic

Lesson Plan for Parent(s)/Guardian(s)

Today, students will be creating an Infographic (visual media representation of information), intended to inform an audience about a theme related to cybersecurity covered so far.

Students will choose one of the following themes related to Digital Citizenship, covered in the unit so far, for their Infographic: *Cyber Respect & Online Kindness*, *Positive Digital Footprint*, *Safe Communication Online*, *Passwords & Passcodes* or *The Truth Online*.

Hook 10 minutes	<i>Greet students</i> <i>Great time to check in about well-being</i> <i>Engage prior knowledge</i>
Learning Goals & Success Criteria 5 minutes	<p>Share learning goals for purposeful learning. Success Criteria let students know what they'll be able to do when they've learned this.</p> <p>Learning goals:</p> <ul style="list-style-type: none"><input type="checkbox"/> I can create an Infographic (visual representation of information) on a theme related to cybersecurity<input type="checkbox"/> My Infographic communicates a clear argument or theme related to cybersecurity<input type="checkbox"/> My design is attention-grabbing
Input & Modelling	<p>Introduce infographics by sharing relevant infographics that students may be familiar with. There are probably infographics all around the school that you can use as examples! Infographics are a special way to use digital media to share a message or a main theme on a topic in cybersecurity. The students will need to choose a theme that matters to them, and create a central message related to Digital Citizenship for their Infographic.</p> <p>Examples of cybersecurity-related infographics are available on the Government of Canada website: https://www.getcybersafe.gc.ca/en/resources</p> <p>Sample infographic:</p>

WE HEARD YOU GOT A NEW DEVICE

Before you start using it, take these steps to customize it and keep it cyber safe.



GET SECURE

- ☐ LOCK YOUR DEVICE WITH A STRONG PASSWORD AND/OR BIOMETRICS
- ☐ ENABLE MULTI-FACTOR AUTHENTICATION
- ☐ REVIEW THE PRIVACY POLICY AND TERMS OF USE
- ☐ UPDATE YOUR PRIVACY SETTINGS



STAY UPDATED

- ☐ UPDATE YOUR DEVICE'S OPERATING SYSTEM
- ☐ ENABLE AUTOMATIC SOFTWARE UPDATES

MAKE IT YOURS

- ☐ UNINSTALL APPS YOU WON'T USE
- ☐ REVIEW APP PERMISSIONS, LOOK OUT FOR ANY APPS ASKING FOR ACCESS TO DATA NOT RELEVANT TO THEIR FUNCTION
- ☐ TURN OFF LOCATION SERVICES WHEN NOT IN USE
- ☐ DISABLE ANY OTHER FEATURES YOU DON'T NEED

ONCE YOUR DEVICE IS SET UP



APPLY A CAMERA COVER



DISABLE BLUETOOTH WHEN NOT IN USE



AVOID CONNECTING TO PUBLIC WI-FI OR USE A VPN



ALWAYS ACCEPT OS AND SOFTWARE UPDATES

	<p>full infographic available here: https://www.getcybersafe.gc.ca/en/resources/we-heard-you-got-new-device</p>
<p>Guided & Independent Practice</p> <p>20 minutes</p>	<p><i>Observe, prompt, support, enrich</i></p> <p>Based on the following themes, students will be creating an Infographic that has a central message. Students must conduct research on that theme and include it in the Infographic. (<i>Themes: Cyber Respect & Online Kindness, Positive Digital Footprint, Safe Communication Online, Passwords & Passcodes or The Truth Online.</i>)</p> <p>Lead students through a brainstorming session, then have them brainstorm independently or in small groups about potential topics for their Infographics (<i>i.e., how to spot a cyberbully, or how to create strong and secure passwords</i>).</p>
<p>Check for Understanding</p> <p>10 minutes</p>	<p><i>Observations, formative assessment</i></p> <p>Once students have brainstormed potential topics, develop Success Criteria for the Infographic.</p> <p>Suggested Success Criteria, or Success Criteria to start with:</p> <ul style="list-style-type: none"> <input type="checkbox"/> I can create an Infographic (visual representation of information) on a theme related to cybersecurity <input type="checkbox"/> My Infographic communicates a clear argument or theme related to cybersecurity <input type="checkbox"/> My design is attention-grabbing
<p>Closure</p>	<p><i>Review, wrap-up, discussion, appreciations</i></p> <p>Choosing the topic: Students can share the topic they chose with their teacher before the end of the class, or it can be shared prior to the next lesson.</p> <p>Using the Rubric, and the Success Criteria, assign the Infographic and provide students with a due date.</p>
<p>Resources</p>	<p>Resources for the Educator</p> <p>Rubric (can be edited)</p>
<p>Assessment</p>	<p>For Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Observation✓ <input type="checkbox"/> Anecdotal notes <input type="checkbox"/> Checklist <input type="checkbox"/> Conferencing/conversations <input type="checkbox"/> Work samples/products <input type="checkbox"/> Check-ins <p>As Learning:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Rubric <input type="checkbox"/> Success criteria✓

	<input type="checkbox"/> Self-reflection <input type="checkbox"/> Other Of Learning: <input type="checkbox"/> Quiz <input type="checkbox"/> Test <input type="checkbox"/> Presentation <input type="checkbox"/> Assignment <input type="checkbox"/> Other product
Notes:	