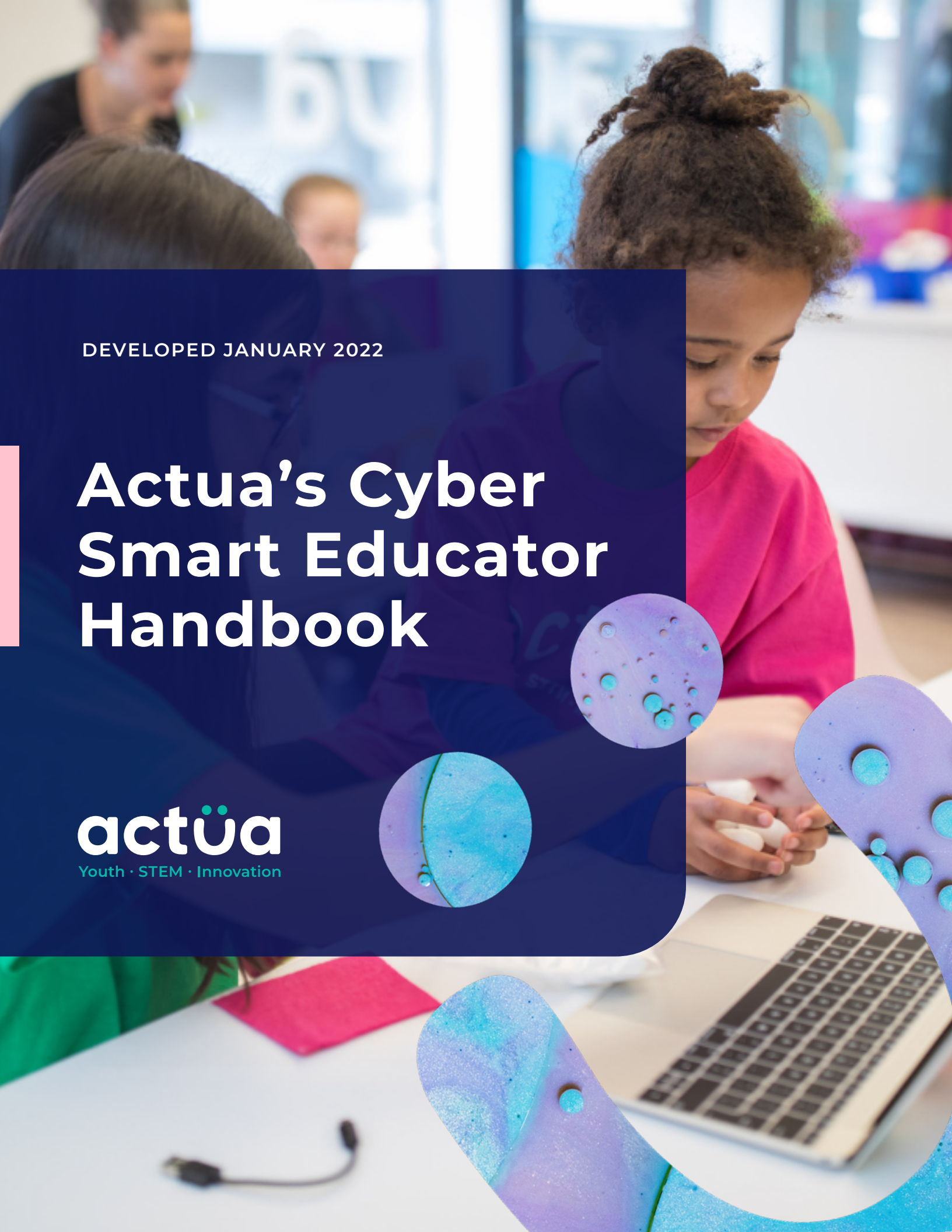


DEVELOPED JANUARY 2022

Actua's Cyber Smart Educator Handbook

actüa

Youth · STEM · Innovation

Table of Contents

About Actua

Actua is Canada's leading science, technology, engineering and mathematics (STEM) youth outreach network, representing a growing network of over 40 universities and colleges across the country.

Each year 300,000 young Canadians in over 500 communities nationwide are inspired through hands-on educational workshops, camps and community outreach initiatives. Actua focuses on the engagement of underrepresented youth through specialized programs for Indigenous youth, girls and young women, at-risk youth and youth living in Northern and remote communities. For more information, please visit us online at www.actua.ca and on social media: Twitter, Facebook, Instagram and YouTube!

Terms of Use

Message from CEO

> **The online world has become an easy place for youth to build connections, express opinions and foster a sense of belonging.**
>
> - JENNIFER FLANAGAN

The pace of digital transformation here in Canada and around the world is accelerating at a rapid pace. Youth are online now more than ever, having had to rely on technologies, such as computers, smartphones and tablets to learn, connect and socialize through the COVID-19 pandemic. There is no off button for many. The online world has become an easy place for youth to build connections, express opinions and foster a sense of belonging. But, while these interactions can contribute to the positive development and well-being of youth, the internet can also be a place where youth fall victim to various online threats, including phishing, fraud, ID theft, bullying and exploitation.

As part of our mission to unlock the infinite potential of youth, we're working relentlessly to remove or confront barriers to youth engagement in STEM. These barriers include cyber threats and attacks which can discourage youth from feeling empowered to explore, create and connect online. For these reasons, Actua believes cyber safety and digital citizenship is an integral part of digital literacy and should be embedded within all digital literacy curricula.

> **Actua's Engage. Empower. Connect. (E2C) project is a cyber empowerment initiative that seeks to build positive digital citizenship from the ground up.**

Our goal is to create a new cyber smart generation ready to embrace the challenges of the digital age. We're supporting youth to understand how to critically assess online interactions, avert online threats and use technology in innovative, healthy and safe ways. We're also helping you, educators,

bring cyber smart education into your classrooms. While this project is built on the foundation of Actua's national coding and digital skills program, E2C is testing a new approach that counteracts the developmental, socioeconomic and tech-based risk factors that make youth, especially girls, vulnerable to the social psychology of the internet.

We ask that you join us and our growing network of 40+ network members in empowering youth with the skills, awareness and confidence to be cyber smart and good digital citizens by adopting this handbook as your guide. You can also find more information, including classroom resources and activities on digital citizenship and cyber safety, at actua.ca.

Sincerely,

Jennifer Flanagan
President & CEO, Actua

Why and How?

Why was this content created?

We are in the digital age — an age when technology like the internet is heavily influencing how we learn and stay connected.

Today, youth are growing up with the unique experience of having endless information at their fingertips. According to Public Safety Canada, Canadians under 25 years old spend an average of 7 hours online every day (Safety in Canada, 2019). This can be startling when compared to another statistic, which is that 42% of Canadians experienced at least one cyber security incident during the pandemic (Statistics Canada, 2020), which has highlighted an increase in cyber threat actors and complexity.

While the digital age offers an environment rich with opportunities, it also presents youth with challenges and threats that can have a negative impact on themselves and those around them. This handbook is one component of Engage. Empower. Connect. (E2C), Actua's Cyber Smart Project, which equips youth with the knowledge, skills and resources needed to navigate the internet safely. The project enables youth to:

- Be empowered digital citizens
- Create positive, inclusive spaces both online and offline
- Make smart and informed decisions when using technology
- Encourage proactive and self-driven formation of online identities
- Leverage cyber smart strategies to solve challenges and mitigate risks faced online
- Identify media bias and misinformation
- Spot and avoid various cyber threats (phishing, malware, etc.)

How to use this handbook?

The E2C Cyber Smart Educator Handbook is designed to support you as an educator in your journey to bring Cyber Smart Education into your classroom. Our goal is to support

you in fostering cyber smart mindsets by sharing insight from experts and providing curated background information to facilitate activities in the E2C series. By using this handbook, you will:

- Gain insight on big topics in cyber safety (online identities, digital citizenship, preventative strategies, cyber threats, etc.)
- Visualize how these elements are relevant to K-12 education and real-world contexts
- Use a constructive approach and empowering language when teaching youth about cyber safety
- Learn best practices to facilitate the “Engage. Empower. Connect.” activity series
- Find additional resources at the end of this document to help you further build your knowledge-base of cyber safety, cyber security, and digital citizenship

Depending on your needs, you might want to jump into this handbook at different points — it is not necessary to read it in a linear fashion. Here are a few recommendations:

- **Looking to learn Cyber Smart fundamentals?** The Cyber Smart Primer for Educators (starting on p. 8) is intended to provide teachers with a brief overview of the fundamental concepts needed to understand cyber safety, cyber security and digital citizenship before bringing it into classroom instruction.
- **Interested in making connections to K-12 curriculum?** Following the Cyber Smart Primer for Educators, this handbook introduces Actua’s E2C Cyber Smart Education Framework on p. 21, explaining how we structure our approach to Cyber Smart Education for K-12 classrooms. This framework provides relevant, actionable steps for implementing the E2C activity series with students.
- **Ready to deliver classroom activities to teach youth to be Cyber Smart?** Start at Teaching Cyber Smart Education (p. 25) to explore Actua’s recommendations for teaching hands-on activities that help students understand the importance of cyber safety, cyber security, digital citizenship and potential career paths.

As you read, we encourage you to think of ways you can incorporate and adapt this content to fit the needs of your own learning environment. Furthermore, we want you to feel empowered to use the internet as another means through which to find (credible and reliable!) resources that can help you grow and customize your own content.

Let’s get started!

Cyber Smart Primer for Educators

Understanding how to use technology in innovative, healthy, and safe ways is at the heart of Actua's STEM programs. That understanding is a central concept to *Engage. Empower. Connect.*

For this project, we define Cyber Smart by combining cyber safety, cyber security and digital citizenship. On a cyber safety level, it is being mindful and proactive about risks while being able to make smart decisions. On a cyber security level, it is the safe and responsible use of information and technology by understanding tools, processes and practices used to protect personal data and keep networks secure from unauthorized access or attacks. On a digital citizenship level, it is also about being responsible with information we find and share online, upholding respect and inclusion through netiquette, and thinking critically about our future role and contributions online. Together, this can foster youth that are both cyber smart and cyber safe.

In this section of the handbook, we will provide you with a rationale for why cyber safety education is essential for youth. It will also explain several of the key concepts, challenges and topics that develop when discussing cyber safety. Finally, it will explore how to effectively bring Cyber Smart education into your learning environment.

Cyber Safety for all Canadians

Why the shift to cyber safety and security?

1. EMPHASIZED NATIONAL FOCUS

Understanding Cyber Security and the skills, tools and mindsets that are required to be safe and healthy online is critical for all Canadians, especially as we spend more time online and cyber threats become more complex (Canadian Centre for Cyber Security, 2020). Public awareness and education are some of the most essential ways to strengthen national and individual security. In 2018, the importance of Cyber Security

education was emphasized when the Canadian Ministry of National Defense announced the official launch of the Canadian Centre for Cyber Security and the National Cyber Security Strategy. The Canadian Centre for Cyber Security emphasizes the importance of a national focus by describing cyber defence as a team sport, "Government, industry, academia, and civil society must all work together to strengthen Canada's cyber security" (Canadian Centre for Cyber Security, 2021).

2. PROTECTING AND PREPARING YOUTH

Being online can be risky, but it can also have immense value. In addition to our national focus, we know that youth and educators are working to build digital skills, as well as developing healthy online behaviours in order to be prepared for the digital future. Youth need to learn about the various cyber threats that exist online and strategies to avoid/appropriately deal with these risks. Learning how to be cyber smart can help youth protect themselves online, as well as allow them to share insights with their families and peers.

Youth should have opportunities to feel empowered and skilled in these areas, and explore potential careers in cyber security which have grown in need and number in the past few years. According to the Canadian Centre for Cybersecurity, cyber security professionals are in demand with the number of jobs growing by 7% every year in Canada and with 3.5 million vacant positions worldwide in 2021 (Cyber Security Career Guide, 2021).

3. EMPOWERING YOUTH

Historically, this information has been taught from a fear-based and deficit-based approach. This approach can instill feelings of fear, marginalization, and helplessness when youth learn about the potential risks and consequences they face online. Making youth afraid of using digital platforms is not how we want to develop digital citizenship. In addition to learning about online risks, youth should also learn about the positive opportunities of being online. We want them to feel empowered to seek out information online and have the digital skills to make sense of what they encounter. They are capable of creating inclusive environments online and understanding how to recognize and avoid cyber scams that threaten their personal data.

Rather than using negative stories that portray youth as victims of cyber threats, this handbook explores prosocial norms that demonstrate good digital citizenship and appropriate online behaviours. Treating youth as though they are unable to protect themselves may lead to youth feeling disempowered, disengaged, and disconnected. The need for an approach that does not victimize youth was a motivating factor for our "Engage. Empower. Connect." activity series, as well as this E2C Cyber Safety Educator Handbook.

Being Online

How would you describe the internet? How do the various characteristics of the internet impact who we can be online?

The internet allows individuals to communicate in unique ways. For example, they may share thoughts and ideas anonymously, respond to direct communications without time constraints, and easily reach people they do not know in real life. This has come to affect the way people interact and socialize online relative to the way they might interact and socialize offline.

We are also experiencing online and offline environments coming together in ways that are hard to separate. Someday soon we may understand all spaces as a type of online/offline hybrid.

Smartphones and other network connected devices can travel anywhere. Our cars, TV, gym equipment, traffic lights, schools, and other infrastructure and machinery often connect to the internet, networks, and one another. Inevitably, this shapes how we interact with each other, technology and the world.

Here are some of the key characteristics of the internet to understand and shape the way you can talk to your students about the importance of cyber safety:

The Internet is...

- **Global and Always On.** Without restrictions, there is instantaneous and constant access to content from every part of the world 24/7, including massive amounts of both information and misinformation. The internet is always "on", this means that yes, you can access information anytime... but anyone can also access your personal information at any time. Additionally, the ability to access whatever, whenever, has reduced patience and resilience. Today's internet users no longer have to wait for something to become available, or to sit through an episode of something they don't like. They are able to simply click and pick something new.
- **Interactive.** We can participate and interact with the internet and others who are online
  - → **Think:** social media posting, sharing research, entering into virtual gaming sites.

- **Anonymous.** Online anonymity, or perceived anonymity, can loosen typical social norms as our reputations are not at stake. This can have benefits (e.g. seeking out and engaging with communities our typical social circle would not approve of, finding new communities of support online), but may also facilitate negative behaviour online
    - → **Think:** comment threads on videos or blog posts, language or harassment that folks would not make face-to-face.
- **Addictive.** Certain features of the internet are designed to keep us spending time and money, playing games, watching content and sharing information. The fun and addictive nature of the internet is not accidental and many profit from our use of connected devices. When we are able to remember that much of the internet is designed to learn from us and sell products or ideas to us - we are able to more critically assess the time we spend online and which ways we are engaging with technology. The effects of social media on people, particularly youth, is only beginning to be explored.
- **Crowd-sourced.** A lot of diverse information can be posted across multiple media forms. This information can be republished (reshared, retweeted, reposted) with a scope that is as wide or wider than the original publication.
    - → On a negative note, this can lead to a skewed sense of what is worthy of attention. On a positive note, it can result in a quick diffusion of important information across networks. Regardless, a critical approach to consuming internet-based media (e.g videos, articles, images) is absolutely fundamental for online safety.
- **An Echo Chamber.** The internet has many online spaces, like comment boards or social sites, in which a person encounters only beliefs or opinions that coincide with their own. This can mean that the user's existing views are consistently reinforced. Being online and unaware of these echo chambers can mean we are not exposed to alternative ideas, diverse opinions, or even evidence-based research in some cases. The internet can be a great place to find like-minded communities, but it can also be a frightening place where the powerful forces of groupthink can easily manipulate your opinions. Machine learning has a major role here - based on a user's activity, the internet learns their preferences and feeds them more of what they want to see. This can be great for leading us to information or communities we are interested in or seeking out, but can be very limiting and even dangerous
    - → **Think:** Social media 'showing' you TikTok videos that you find funny or "perfectly tailored" to you, targeted advertisements, invites from unknown groups that are similar to other groups you belong to
    - → **Caveat:** Machine Learning is designed to do what the developers intended, not what's best for you. Those developers may want to show you more ads or could try to sway your opinion.

Overview of Key Topics in Cyber Smart Education

What different elements are associated with cyber safety and cyber security?

1. DIGITAL CITIZENSHIP

Digital citizenship is the ability to understand and engage with the internet at an appropriate level. As digital citizens, we spend time working, learning, and socializing in connected online spaces. In these spaces, it is important to know what information should be kept private, how to create positive and inclusive connections, and how to be critical when assessing information online. In addition, there are many different risks to be aware of in order to mitigate or avoid them, including data breaches, online bullying, phishing scams, misinformation, age inappropriate behavior and content, and identity theft.

> **Cyber smart digital citizens use technology in safe and effective ways.**

This includes having an understanding of **Digital Security**, **Netiquette**, and **Digital Health and Wellness**. A good digital citizen demonstrates critical thinking, leadership, kindness and responsibility.

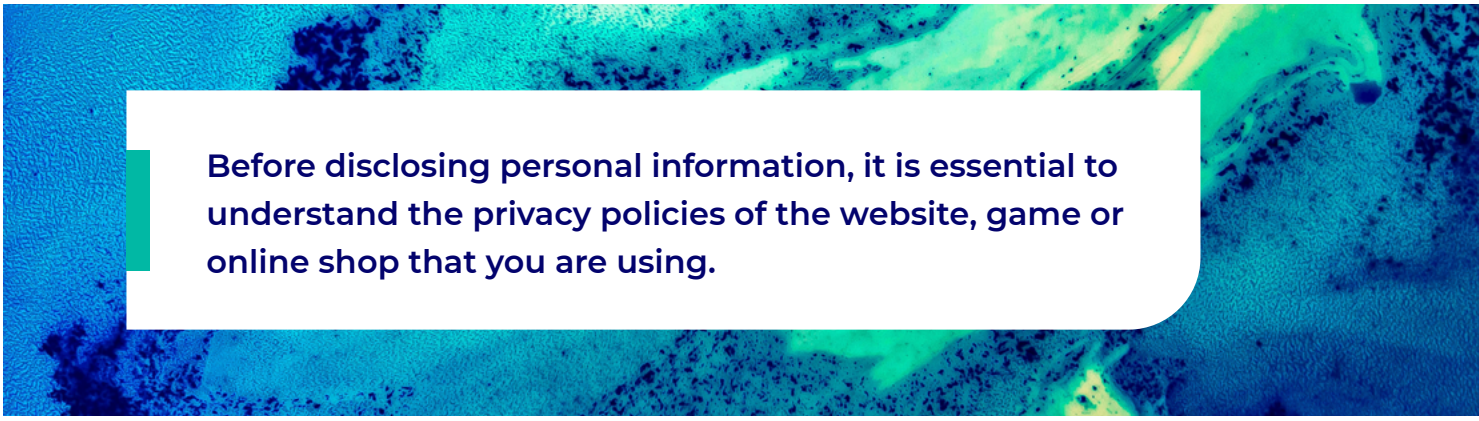
2. ONLINE IDENTITIES & DIGITAL FOOTPRINT

When we use connected devices, we are developing an online identity. Social media platforms, gaming profiles and other interactive content are some of the ways we express ourselves online. Online identities differ in both big and small ways from our “real life” identities. As youth explore their identities and personal values, playing with

online personas can be tempting - and potentially dangerous. It's important to be conscious of the fact that most, if not all, of our online actions contribute to our permanent digital footprint. Online identities are also made up of data we can't access. For example, Fitbit collects data about how often you exercise, and Netflix collects data about the types of shows you watch. They may then tie this information to what they think about you as a person. All connected devices add to your digital footprint.

3. ONLINE IDENTITIES & DIGITAL FOOTPRINT

As the number of websites and tools asking for personal information rises, so too does the risk of our data being accessed by others. Using critical thinking and cyber smart skills to assess a particular situation's risk can be a game-changing practice for being smart with personal information.



Before disclosing personal information, it is essential to understand the privacy policies of the website, game or online shop that you are using.

Rather than quickly accepting the Terms of Service, it is good practice to read it and reflect on the privacy policy you are agreeing to (see Being Aware of Laws, Freedoms and Responsibility in Cyber Safety p. 19 for more information).

For example, a music streaming platform, an online registration form for an upcoming webinar you would like to attend, and a free gaming site might all ask for your date of birth. However, they will likely all have different privacy policies, and might store and share your personal data in different ways. Think of it this way: your payment for the product is often your data — it is important to consider if the product or service is worth that much of your personal data.

4. DIGITAL HEALTH AND WELLNESS

Mental health and wellness is important offline and online. It is important to be aware of what content you are consuming online, as well as just how much time you're spending on connected devices.

> **It is important to do regular check-ins with yourself by taking a moment to consider how you feel after a certain event or even after spending a lengthy amount of time online.**

This can help you to assess your wellness and relationship to the internet. Providing youth with opportunities to reflect — as well as teaching self-awareness and check-in strategies — is a way educators can support building positive digital health patterns for students.

5. CYBER SCAMS AND CYBER CRIMES

Cyber scams and cyber crimes range in complexity and severity. Crimes such as hacking, identity theft, and child exploitation are punishable by law. Other cyber crimes are more commonplace and can be encountered almost daily, such as phishing attempts. Many of the attempts to steal personal, financial, or intellectual data are obvious - like a flashing 'Free Cruise!' pop-up. Others can catch us off guard, such as a message saying 'Win an iPhone for completing this survey' that appears on a trustworthy site. Finally, some are very believable and look indistinguishable from legitimate communication, such as an email from a familiar sender prompting you to update your "compromised" password.

Best Practices for Cyber Safety

1. Review, use and understand your privacy settings.
2. When possible, keep personal information limited to only what an app or service requires.
3. Trust, but verify. Remember, the internet is not always as it seems.
4. Use secure Wi-Fi connections (and when connecting to an insecure network, avoid logging in to accounts and use a reputable VPN).
5. Avoid malicious downloads by thinking before you click, download or accept
6. Strong passwords and password management are essential.

7. Everything online should be considered permanent and potentially public. It all adds to your digital footprint.
8. Always apply updates to your software. Use malware and virus protection.
9. In online personal spaces (Instagram, Snapchat) connect only with people you know in real life or do not share personal information (e.g. your name, address, or birthdate).

Risks Youth Face Online

Youth should be aware of the benefits and risks that technology can introduce. The risks that youth face online include all the same risks, scams and crimes that adults can experience.

In addition to these risks, it is possible for youth to encounter threats such as child exploitation, sexting and cyberbullying. Nobody wants to feel uncomfortable, worried or exploited, so creating a safe space to talk about these feelings can be one way to initiate conversations about online risks.

What types of risks do youth face online and how can educators help mitigate and educate youth about these risks?

SECURITY AND PRIVACY ISSUES

It is common for youth to share passwords and passcodes with their friends and peers without understanding the risks associated. While exchanging these digital details can be seen as a trust exercise, it also poses security and privacy issues due to the nature of someone else having access to your account or profile (Kaspersky, 2018).

If youth reuse the same password and username, it is possible for others to use credential stuffing to access other accounts.

In addition, many youth will access the internet using a family computer or tablet device. This means they can potentially access credit card information and auto-saved passwords — and so can those looking to access that information. On the other hand, sharing devices means that a whole family can benefit once one member learns how to be cyber smart!

WHAT CAN YOU DO AS AN EDUCATOR?

It may seem tempting to share social media or gaming passwords. Even library log-in information can seem fine to share with peers, but it is NEVER a good idea. It can be helpful to remind students of this when they log into their student accounts on shared computers, or even on personal devices.

CHILD IDENTITY THEFT

It may not seem likely that hackers want to steal a child's personal information, but child identity theft is on the rise. If youth post enough personal information publicly online, a cyber criminal can access this information and commit crimes in a child's name or create financial issues that go undetected until much later — like when the child eventually applies for a line of credit. This can be prevented by being very cautious about sharing personal information like your full name, birthday, and address.

WHAT CAN YOU DO AS AN EDUCATOR?

Avoid using sites that require students to create accounts that share personal information. Remind students that when they are accessing new sites, whether at home or at school, to consider why they're being asked to share information and to not disclose personal information, or to use an alias or nickname rather than their full name. If it is not required by an official site, they can falsify their birthday - for example on a game registration.

OVERSHARING

There is an inherent tension on social media between conserving privacy and sharing one's experiences with the community. Given the pervasiveness of social media (especially within younger generations), youth often tend to favor community connectedness over privacy.

> **Youth may have an attitude of "I have nothing to hide" or "I don't do anything bad/illegal online, so why should I care who sees my digital footprint?".**

Privacy isn't about what you have to hide. It's about owning the data that belongs to you and having control over what people can do with it.

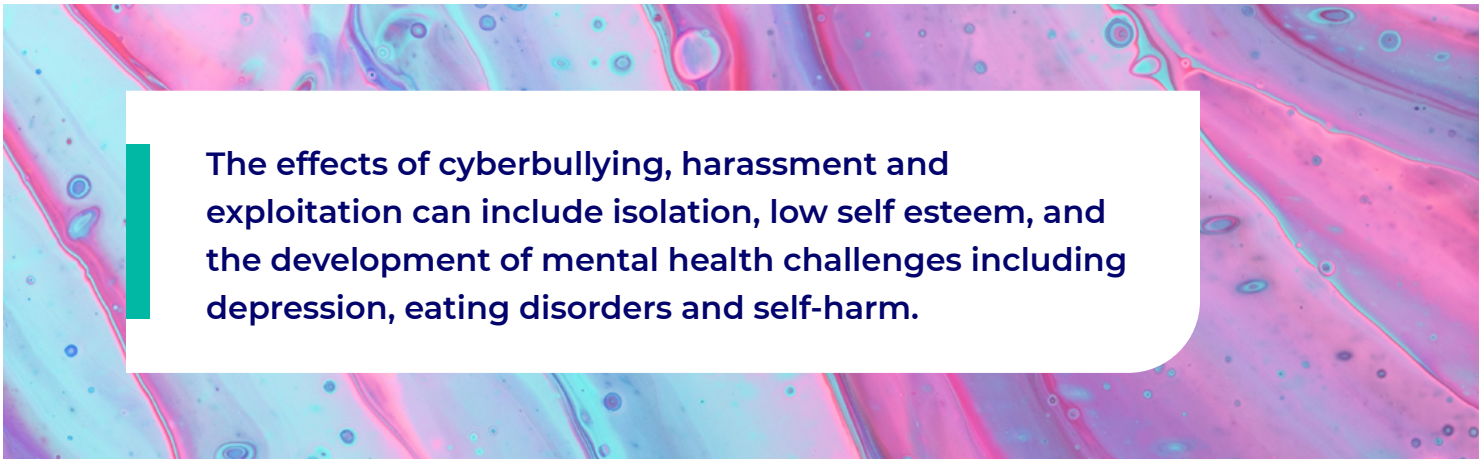
WHAT CAN YOU DO AS AN EDUCATOR?

It is empowering to explain to youth that their online information consumption and identity creation are things they have control over, but this needs to be done thoughtfully and by making the most of Privacy Settings. Introducing them to concepts of oversharing and personal data can help them to understand privacy more and the impact of a privacy breach. Questions to ask: What information should be kept private? Who needs to see this information? Do you know who you are sharing this information with?

CYBERBULLYING, HARASSMENT, AND EXPLOITATION

Cyberbullying remains a serious and pervasive issue for youth. Cyberbullying is more than making hurtful comments online - among other examples, it can look like spreading rumors through text message, creating a fake social media account and pretending to be someone else in a bad light, forwarding an embarrassing photo of someone, sharing intimate photos that do not belong to you, or trolling/stalking someone online. Often cyberbullying can be downplayed, but the acts categorized under this term can include distribution of child pornography (e.g. sending personal compromising photos/forwarding intimate photos of someone under 18, even if to other teens), extortion, harassment, slander, or domestic violence.

This type of bullying is often persistent but subtle, where an outsider who sees this behavior online may not even know it is harassment due to inside jokes or comments between youth that are derogatory or demeaning.



The effects of cyberbullying, harassment and exploitation can include isolation, low self esteem, and the development of mental health challenges including depression, eating disorders and self-harm.

WHAT CAN YOU DO AS AN EDUCATOR?

Include cyberbullying in conversations about bullying more broadly, and discuss what students are seeing — and how they are managing it. Many of the same strategies used to tackle bullying can be applied to online environments. Cyberbullying can happen outside of school hours (with peers or strangers) and students need to understand how to identify when cyberbullying or harassment is happening. They should also be aware of what steps they can take to protect themselves and others from it, or understand how their own behavior can be perceived as cyberbullying. Help them discover safe places to report bullying, including directly on the social media sites they use.

Create opportunities for students to talk about their experiences with online interactions and encourage them to do wellness checks when online. Since youth can be both the victim and the cyberbully, they should ask key questions of themselves: Do I feel good after talking to this person? Am I comfortable with the kinds of questions they are asking me? Am I proud of how I treated this person? Would I want everyone to know it was me who wrote that comment?

SOCIAL PSYCHOLOGY AND THE INTERNET

Interactions with others online can play off of human emotion - but so can your interactions with the content and information you post, come across or actively view. For example, the 'like' button is a perfect example of how emotion and social psychology are linked to our time spent online.

> **Our minds have chemical reactions when we get positive interactions on social media such as 'likes'.**

Conversely, we can experience "let down" in our bodies when our content is not validated. Youth have a wealth of information at their fingertips which can influence how they want to look or act - for example, if they follow many celebrities they might have an unrealistic expectation of perfection for themselves if they don't know to make a distinction between what is online and what is real-life (think: body image, relationship status, wealth, etc.).

WHAT CAN YOU DO AS AN EDUCATOR?

Empower youth to view their relationship with the internet and technology as them using the tools and not the other way around. It is essential to emphasize that youth can and should control their online activities, presence, and legacy. Focus on the far-reaching impact of what they do, the way the world sees them through digital footprints, and the permanence of what is left behind.

Being Aware of Laws, Freedoms and Responsibility in Cyber Safety

What law, rights, freedoms and responsibility might be important for Canadian youth to be aware about?

We are covered under many **privacy laws in Canada that are intended to protect Canadian citizens and their privacy** - for example, there are laws that exist for government institutions like schools, laws for consumer applications, and laws for health data. These laws are overseen by Privacy Commissioners. We have one Privacy Commissioner that oversees all of Canada and individual Privacy Commissioners in each of the provinces. New versions are anticipated to be released in the next few years that better reflect how far technology has come. In Canada, **we have the right to request a copy of our data**. That means that you can contact a company and ask them to share with you everything they have recorded. This happened in 2020 when an individual asked Tim Hortons to share the data that they had collected about him from the device application. He was shocked to find that they were tracking his location at all times and not just when he made the order. This tracking was against what the privacy policy said they did, so he was able to file a complaint with the Privacy Commissioner.

> **Most of the apps and services we use come from the United States (e.g. Google and Facebook).**

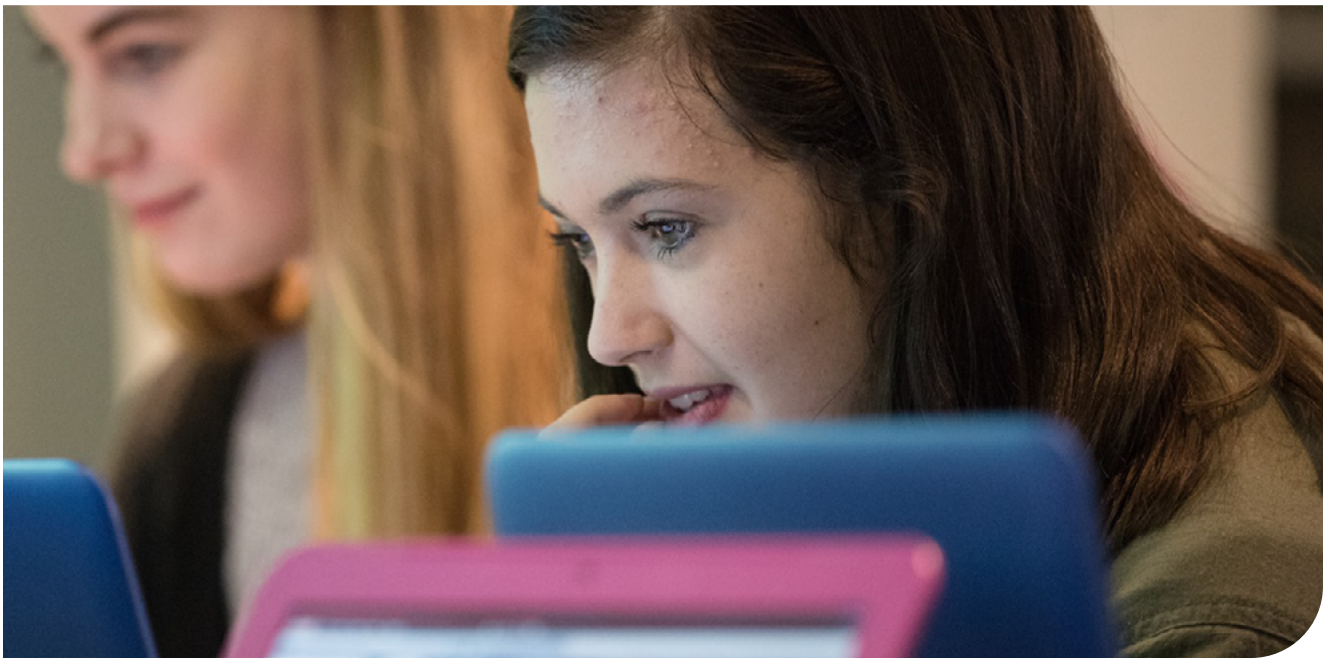
Though we do have some rights as Canadians, we are still under their laws when it comes to the US government being able to access our data because it is kept in the US. If you live in Europe you fall under a legislation called GDPR, or the General Data Protection Regulation. This privacy regulation is currently one of the strongest in the world. It puts individuals first and even allows people to request their own deletion from a system - this is a privacy regulation we hope to get in Canada.

WHAT ABOUT YOUTH?

It is important to note that in most cases, collecting data from a child under 13 is prohibited unless the application or service is designed for this purpose. For example, Instagram is only legally approved for use by youth 13 and up (because of advertising and re-selling of data) whereas Google for School is made for children (does not collect or resell data). It is important that educators, parents and youth select apps and services that are targeted for them. If not, youth are at risk of having more data collected about them than they are aware of. For youth over 13, they need to understand the risks of what they have agreed to in the Privacy Policy and Terms of Service of a product or service. Most youth, or even adults, do not read these documents.

The Privacy Policy explains what personal data the app or service collects, why they collect it, what they do with it, and who they share it with.

The Terms of Service explains how the product or service operates and how you are expected to interact with it. If anything is prohibited by the application then it will be listed in the terms along with the consequences of breaking these terms. It is important that all internet users have a basic understanding of the trade-off or payment with data. No service is free. If you are not paying for the product then you are the product.



Actua's E2C Cyber Smart Education Framework

Actua's Cyber Smart Framework was created in early 2021 in collaboration with Cyber Security professionals, law enforcement leaders, educators, and other experts in the field.

This Framework guides the approaches of Actua's E2C Project and informs content development, while providing other educators with an overview of key concepts and learning outcomes for a cyber smart education.

An online, downloadable version of the English and French Framework is available on actua.ca. You can also find both versions below.

Perspectives Informing the Framework

Youth are curious, looking to form connections, explore and define their identities and interests. Friendships and other relationships are paramount at this age, and key influencers like family and friends are a big part of decision making. These defining adolescent traits are not inherently negative (in fact, they are incredibly valuable!), but can put youth in a risky place if they are not aware of safe practices when online.

Youth are subject to specific risk factors that make them particularly vulnerable to social pressures, online victimization and cyber insecurity. Young adults are in the process of developing their personal and social identities, and this search for meaning or belonging could lead them to being at risk for dangerous online behavior personally as well as susceptible to risky behaviors online from others; from peers to hackers to social pressures to phishing scams to false information. The goal of this framework was to determine how to equip youth to be responsible, digital citizens that recognize different risks and know the strategies to be smart and safe online.

Actua's Cyber Smart Framework

	Engage	Empower	Connect
Big Ideas	Equipping youth with tools (knowledge) to build cyber safety is fundamental to fostering responsible use of technology.	Practicing skills, applying and translating knowledge into action and/or creation builds a cyber smart generation.	A cybersmart mindset relies on positive communities and healthy relationship building both online and offline, and builds leadership for continuous learning, critical thinking, and identifying supports for continued safety online.
Themes	• Cyber security • Online identity (e.g., credential stuffing) • Data and online information • Privacy, virtual private network (VPN)	• Data connections to artificial intelligence (AI) • Credibility, bias and misinformation • Intent of online interactions, protection and harm reduction • Open source intelligence gathering	• Self-Expression • Social behaviour & healthy relationships • Interactivity/Network-Oriented Platforms • Community building, global connectivity
Learning outcomes (Students will...)	• Understand digital literacy and demonstrate personal responsibility for consuming technology. • Articulate benefits to understanding, using, and creating with technology. • Identify risks when navigating online and/or connected contexts (e.g., IoT), and appropriate actions to mitigate risks. • Build fundamental understanding of digital environments so that youth are informed users of tools, not manipulated by the tool and a l ck of insight into the tech and/or data that drives them.	• Practice cyber safe behaviour through various proactive behaviour (e.g., creating strong passwords, avoiding release of personal information/breaches, etc.) • Identify biased data sources and identify reliable sources of online information. • Articulate intent of indiviuals and groups online.	• Develop a healthy sense of identity, both online and offline. • Understand appropriate interactions with others online, including preventing cyber bullying and avoiding harm. Leverage technology to build positive social networks. • Promote safe behaviour online, including protecting personal information, positive social interactions, and appropriate connections with strangers • Know rights, and identify who/where to turn to for help in cases of compromised safety.
Curriculum connections Synthesized from the Pan-Canadian K-12 CS Education Framework	**CYBERSECURITY** : Defining cybersecurity; making safe passwords using effective criteria; Describing common cyber attacks and malicious content and assessing; Applying prevention practices. **DATA (DATA GOVERNANCE)**: Understanding how digital data is created through digital and physical activity and thinking about who owns the data they produce; Thinking about and using privacy settings in online platforms. **TECHNOLOGY AND SOCIETY (ETHICS, SAFETY & THE LAW)**: Identifying strategies to protect their personal data and identity online; Explaining privacy concerns; Assessing the effects of digital crime on self and society.		

Framework Elements

Big Ideas

The Framework is based on three core pillars: Engage, Empower, and Connect — each with an associated "big idea". **Engage** is all around building a strong base of cyber safety fundamentals, and priming youth with the essential knowledge and tools to stay safe online. **Empower** takes that knowledge and applies it to a variety of situations and contexts. And finally, the **Connect** big idea speaks to the need for youth to build healthy relationships, both on- and offline.

Themes

Under each big idea, there are several themes that support the instruction of each big idea — Engage, Empower, or Connect. These themes are the broad topics that teachers or instructors could tackle as part of an education for that big idea.

The themes are open enough to encompass a wide range of ages and abilities, from novice through to expert, depending on how deep the instruction goes and to what level of technical difficulty.

For example, "data and online information" (a theme for Engage) could be introduced as a username and password at the elementary level, but by high school, students could be learning about big data, how datasets inform algorithms, and how personal information can be used by companies to inform product decisions.

Learning Outcomes

Just as the big ideas lead to several themes, the themes lead to more specific learning outcomes. The Framework's Learning Outcomes are critical goals for learners engaged in cyber smart education and learning. While we do not expect young learners to grasp all of these learning outcomes, the goal would be that by the completion of high school (i.e., upon graduation), a basic cyber smart education would entail all youth achieving these outcomes. These are considered the most fundamental and important skills and knowledge for individuals to stay safe online, regardless of their technical knowledge. In fact, these outcomes were designed to meet the needs of non-technical, non-computer science students — i.e., no coding or computer expertise is required to grasp these concepts.

Curriculum Connections: Bringing Cyber Smart Education into K-12

At the root of the **E2C Cyber Smart Education Framework** is the overarching goal for all students to have sufficient knowledge of Cyber Security, be able to engage in discussion on these topics and issues, be able to think critically while online, and be conscious of career opportunities in this field. Actua's Cyber Smart Framework is designed to directly align with three key areas in the Pan-Canadian K-12 Computer Science Framework:

1. **Cyber Security**
   - → Skills/Practices: Define Cyber Security; make safe passwords using effective criteria; describe and assess common cyber attacks and malicious content; apply prevention practices.
2. **Data (Data Governance)**
   - → Skills/Practices: Understand how digital data is created through digital and physical activity; think about who owns the data they produce; use privacy settings in online platforms.
3. **Technology and Society (Ethics, Safety & the Law)**
   - → Skills/Practices: Identify strategies to protect their personal data and identity online; explain privacy concerns; assess the effects of digital crime on self and society.

By positioning Actua's Cyber Smart Framework within the Pan-Canadian K-12 Computer Science Framework, we offer a roadmap that highlights cyber safety, cyber security and digital citizenship within computer science classrooms, as well as beyond into other non-technical subjects.

Teaching Cyber Smart Education

In combination with the Cyber Smart Framework, Actua has created an activity series with hands-on, interactive activities to help educators reimagine Cyber Smart Education.

Key Tips on Engaging Youth

1. LANGUAGE MATTERS!

- Empowering vs. Deficit-Based: It is crucial to approach this discussion with empowering language so that youth are not afraid to be online. Yes, we want to make them aware of the risks, but by teaching them key skills we help them to build confidence to navigate online spaces in a smart and safe way.
  - "The internet can be a good resource" vs. "The internet is scary"
  - "It is important to ask the right questions" vs. "You need to be on guard and ready to protect yourself"
- Use Prosocial Norms: Research demonstrates it is more impactful to discuss examples of good online decisions, rather than drawing attention to controversial cases or negative consequences to demonstrate the importance of being safe online.

2. START ASAP

- There is no time like the present. It is critical to introduce these topics as early as possible — but be mindful that the content is presented in an age-appropriate way. This means that you, the educator, will also need to familiarize yourself with this content. This handbook is a great place to help you get started.

3. CREATE A SAFE AND WELCOMING SPACE TO HOLD THESE DISCUSSIONS

- Fostering a space where students feel safe sharing their experiences with anything (not just their internet habits) will mean they are more open to discussing issues instead of keeping it to themselves.
  - Maintain open dialogue (this should not be the first, or last, time they share their thoughts!)
  - Share your experiences too (be relatable)

4. BE CREATIVE — FIND WAYS TO EMBED CYBER SMART EDUCATION INTO YOUR CURRICULUM

- As stated above, begin by familiarizing yourself with Cyber Security so you can develop connections to your own content.
- Ideas:
  - Introduce these topics whenever students are using an internet-based activity (ex. Bias and Misconceptions)
  - Begin every class with a small activity and tie it into class discussions at various points of the day.
  - Integrate these topics into different areas of the curriculum to provide multiple opportunities for reinforcing positive online behaviour and addressing problems.
  - Extension activities in each of the six modules provide opportunities to adapt it to older grade levels.

5. FOCUS BEYOND CYBER VICTIMIZATION, AND TOWARDS RESPONSIBLE DIGITAL CITIZENS

- Learning about online safety and Cyber Security is more than just learning about online dangers.
- We want to encourage students to be well-rounded and responsible digital citizens, meaning that we want to help them understand how to effectively and appropriately use digital technologies.

6. ENCOURAGE STUDENT CONTRIBUTION & COLLABORATION

- Trends and technology are constantly evolving, and youth are often more aware of what is current than teachers are.
- To help stay on top of cyber trends, create a space where youth can share their digital knowledge and perspectives with each other and collaborate to solve problems. Encourage peer-based discussions, listen to what they are saying, and adapt your content to match their needs.

7. FOSTER EMPATHY

- As youth learn to navigate the world, they may experience personal challenges (identity crisis, friendship or relationship dissolution, academic challenges, feelings of injustice, wanting to fit in, feelings of isolation, image challenges (ie. eating disorders, dysphoria), and possibly many others). This is important to keep in mind as we look to teach youth about safely navigating online experiences and forming relationships with others and the self.
- Empathy is as important offline as it is online, and is a key tool in addressing harmful online activities.
- While it can be challenging to develop online empathy for various reasons (perceived lack of consequences, anonymity, misinterpretation of reactions, disinhibition), that does not make it any less important. Individuals often create a separation between online and offline activities. However, they aren't separate, and we need to begin to break down that myth. It is important for youth to understand that their online actions do have an impact IRL (in real life).

8. BE CLEAR AND EXPLICIT ABOUT DEFINITIONS

- Youth may already have some established misconceptions about several terms in this content. It is important to be explicit and provide diverse, clear examples for terms being introduced.
- According to Bazelon (2013), it is important to avoid labelling. For example, few will willingly take on the label of "victim" or "bully". Instead of openly discussing their actions (even if it fits within the definition), youth may deny them because of the stigmatization and emotional impact of those terms.

9. ACKNOWLEDGE THAT NOT ALL YOUTH HAVE DEVICES

- It is important to recognize that access to devices and to the internet varies. Some youth can access the internet using a family computer or tablet device, some may only have access at school, others might have their own device.
- Be mindful of this when you frame your discussion - it will be helpful to learn about what their experiences online are like.

10. REPRESENTATION AND RELEVANCE MATTER

- Review the content and find ways to make it more relevant to the students in your class. Create additional opportunities for students to see themselves and relate.
- Examples:
  - Swap in articles for students to analyze that are relevant to their communities (Activity: Web Detective)
  - Encourage all students to represent themselves in the visuals they create at the end of every activity (posters, infographics, etc.)
  - Find diverse individuals in the Cyber Security field to share with your class.

Glossary

Term	Definition
Antivirus Software	Software that defends against malware by scanning programs to learn if they are harmful.
Bias	Having an already formed opinion to support or oppose someone or something in an unfair way. This is often based on previous experiences of what a person judges to be good or bad.
Caesar Cipher	A simple form of encryption where characters in a text are shifted over in the alphabet by a specified number of spaces with a "key." This "key" is also used to decrypt. **Example:** The phrase "bcd" is encrypted with a key of 1 and so it becomes "abc." To decrypt the phrase shift the characters back the other way specified by the key.
Clickbait	A link with a title specifically meant to capture someone's attention. These links usually have no substance and are riddled with ads that can lead to viruses. **Example:** You Won't Believe What This Celebrity Did!
Credential Stuffing	A type of cyberattack where there is the injection of breached or acquired username/passwords into multiple platforms to fraudulently gain access into user accounts.
Cryptography	Cryptography is the process of taking text written in regular everyday language and converting it into a secure code that can only be unlocked by someone it is meant for.
Cyberbullying	A form of bullying that is done exclusively over the internet. It has a very negative impact on the mental health of victims.

Term	Definition
Cyber Security	Similar to household security; Cyber Security is concerned with keeping unknown individuals out. The difference is Cyber Security is meant to protect digital information. This is done in many ways with many different tools.
Cyber Smart	A cybers mart individual is one who is confident in their skill with computers and with the internet, and is capable of being a confident **Digital Citizen** and knows how to navigate the internet in a safe and appropriate way.
Data Backup	The process of creating a copy of the data on your system that you use for recovery in case your original data is lost or corrupted (some examples include using a USB, an external drive, or Cloud storage).
Database	Databases are a collection of organized information. This allows it to be easily accessible in a variety of ways such as specific commands. A good amount of database security prevents data being lost or compromised.
Decryption	The act of decoding a message so that it is readable by the recipient.
Deepfakes	Artificially created audio and visual representations of people that look and sound as if they were real.
Digital Access	Digital access is the ability to fully engage with the internet and with technology. Digital access can be disrupted by lack of access to the internet, lack of disability accommodations, and more.
Digital Age	Marked by the introduction of personal internet devices in the early 2000s, the Digital Age (also known as the Internet Age) refers to the period of time in which access to the internet is readily accessible to most, and has become an integral part of societal function.

Term	Definition
Digital Citizenship	The ability to understand and engage with the internet on a safe and appropriate level, including an understanding of **Digital Security, Netiquette,** and **Digital Health and Wellness.**
Digital Commerce (e-commerce)	Buying and selling goods and services over the internet, oftentimes having them shipped directly to your house.
Digital Communication	The ability to send and receive information with other individuals across the internet almost instantly, regardless of distance.
Digital Health and Wellness	The physical and mental wellbeing of an individual with regards to the internet. Online interactions and information can either improve or detract from digital health.
Digital Literacy	The ability to navigate technology and the internet, and operate with an understanding of how it functions. As well, the ability to create and analyze online information with critical thinking skills.
Digital Rights and Responsibilities	Digital rights refers to the basic right and freedom to use all digital technologies and the internet, while digital responsibilities refers to the responsibility you have to use that technology in safe and appropriate ways.
Digital Security	The protection of information on the internet, and how difficult it might be for malicious individuals to steal or use that information. See also Cyber Security.
Encryption	The act of encoding a message so that it is unreadable to everyone except to those with the key to unlock it.
Fake News	The intentional spread of misinformation to mislead in order to make financial or political gains.

Term	Definition
Hashing	Hashing is a form of one-way encryption used by websites and applications to protect sensitive information such as passwords. It is designed in a way to not be decrypted, rather, it creates a unique number that a website or application can reference.
Imposter	When someone is pretending to be someone they are not. Usually happens when someone is engaging in fraudulent activity.
Malware	Malicious (harmful) software designed to get into a computer without the owner's consent, often with the goal of causing destruction. **Example:** Virus, Worm, Ransomware, Trojan, etc.
Misinformation	False or inaccurate information.
Multi-factor Authentication	This is a security process that asks the user to have an additional form of authentication in addition to just a password. This can look like confirmation sent to a secondary email or even a text sent to a personal phone number.
Netiquette (Digital Etiquette)	An extension of the term etiquette which refers to a societal standard on how to act in certain situations. Netiquette is etiquette for the online world.
Personal Data **(AKA Personally Identifiable Information)**	Information that is private and exclusively associated with yourself. about an individual. It includes both uniquely identifying information such as SIN card or phone numbers, and other descriptors such as medical data, shopping habits, birthdays, or gender.
Phishing	A form of social engineering, this is a tactic used to obtain someone's personal information by convincing them to voluntarily give it up through deception. **Example:** An unknown email contacts you with urgent instructions to click a link to enter your school credentials.

Term	Definition
Privacy	The protection of yourself and your information from being seen or accessed by others.
Ransomware	A type of malware that encrypts your personal files and makes you pay to have them decrypted and get access back. **Example:** You are unable to access your pictures unless you pay $500 to someone.
Server	A server is a piece of hardware that acts as an access point and management system to other resources. **Example:** A game server to allow you to play Minecraft with your friends or a web server to let you access web pages.
Storage	A physical device that stores information that is saved on a computer. There are various types of storage but the most common is a hard drive.
Threats	Also known as “cyber threats”, any digital actions that could lead to harm or theft of information.
Trojan	A type of malware that is disguised inside of legitimate software.
Virus	A computer program with harmful effects that can spread by making copies of itself. These effects can include displaying annoying messages, stealing data or giving other users control over the infected computer.
Virtual Private Network (VPN)	According to Kapserky (N.D.), “a VPN connection establishes a secure connection between you and the internet, where all your data traffic is routed through an encrypted virtual tunnel. This disguises your IP address when you use the internet, making its location invisible to everyone. A VPN connection is also secure against external attacks.”

Term	Definition
Vulnerable (Network)	A device or group of devices that is exposed to a potential attack. This is often due to a lack of security like firewalls and antivirus programs.
Vulnerable (Person)	An individual who is susceptible to online scams and phishing. Vulnerable individuals are those who are more unfamiliar with the internet and don't know how to navigate it safely.
Worm	A type of malware that runs independently and self-replicates to cause damage.

Acknowledgements

Women and Gender Equality Canada

Femmes et Égalité des genres Canada

Canada

ENBRIDGE Fueling Futures™

MOTOROLA SOLUTIONS FOUNDATION

With gratitude to our advisors, reviewers, and collaborators on this work:

- **Abbey Ramdeo,** Actua
- **Caitlin Quarrington,** Actua
- **Cat Coode,** Binary Tattoo
- **Emily Hartman,** Actua
- **Emily N. Cyr,** University of Waterloo

With acknowledgement to the many individuals from groups including Women and Gender Equality Canada, Enbridge and The Motorola Solutions Foundation who provided input that helped to shape this project.

We would also like to offer many thanks to our network members, in particular those who participated in piloting this work in their local communities:

- **Memorial Engineering Outreach,** Memorial University
- **Minds in Motions,** University of Calgary
- **Science Venture,** University of Victoria
- **SuperNOVA,** Dalhousie University
- **Worlds UNBound,** University of New Brunswick

And of course, to the BGC Canada clubs that participated in this pilot.