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 lack 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.		