

Digital literacy – Program

Table of Contents

INTRODUCTION	2
DIGITAL FLUENCY	3
<i>Searching and processing</i>	3
<i>Authenticating information</i>	4
<i>Apps</i>	5
<i>Computing</i>	5
<i>Data</i>	6
<i>Data Backups</i>	6
<i>Data storage</i>	6
DIGITAL SECURITY & PRIVACY	6
<i>Data Sovereignty</i>	7
<i>Data Sharing</i>	8
<i>Cookies</i>	10
<i>Privacy & Security</i>	10
<i>Passwords</i>	10
<i>Digital Viruses</i>	10
<i>Identity Theft</i>	11
<i>Data Collection</i>	11
ETHICS & EMPATHY	12
<i>Digital Identity</i>	12
<i>Digital Awareness</i>	12
<i>Copyright & Plagiarism</i>	13
<i>Harassment & Cyberbullying</i>	13
CONSUMER AWARENESS	14
<i>Phishing</i>	14
<i>Terms of Service</i>	14
<i>Digital Advertising</i>	15
REFERENCES	16

Introduction

Digital literacy refers to individuals' ability to use digital technology (i.e., devices, software, resources) as well as communication tools to "access, manage, integrate, analyze, and evaluate information".¹ The ubiquitous nature of digital devices and information makes digital literacy critical to navigating the modern world. Thus, in an effort to bridge existing gaps in digital literacy within remote Indigenous communities, this culturally-responsive digital literacy curriculum called 'Indigitize' was developed. The objective of this curriculum is to improve the digital quotient and empower youth to contribute to long-term digital innovation in the Metis community of Île-à-la-Crosse.

The program was developed for a paper-based delivery by school educators. The program was developed to be adaptable for various target audiences and geographic locations (e.g., remote Indigenous communities). The format of this curriculum is designed using questions to guide students through the module content. For example, we pose the question "How do I search for information online?" Students are then provided with a response, i.e., "Keyword searching is an effective way to search for information". This format was selected to help students stay engaged.

This curriculum was also created with adaptability in mind so that the content could be modified for different contexts as relevant. The primary way in which educators have the ability to adapt the content is through the use of in-class activities. We have provided areas where we feel that real world examples would be useful to contextualize the information for learners. We have provided starter examples but encourage educators to adapt the examples to fit their context and target audience. We have highlighted these areas using green textboxes.

Curriculum content is organized under the 4 key module headings: Digital fluency, Digital safety and privacy, Ethics and empathy, and Consumer awareness. Each module comprises several relevant subcomponents. Learning outcomes describe the key take-home messages from each module. The learning objectives for this program were adapted from the Digital Literacy Framework for Grades 10-12 developed by the Ministry of Education and Child Care of British Columbia.¹ Module content refers to the key topics covered in each section. As the primary audience for this curriculum is youth in Canada, content was sourced from Canadian sources (e.g., Office of the Privacy Commissioner of Canada) where possible. In-class activities are suggested for each module, describing discussion questions and scenarios to explore in a classroom setting.

Digital fluency

Learning outcomes

- Ability to search in a systematic way for information specified in a web search query
 - Ability to use a variety of searching strategies to conduct effective and efficient online searches
 - Ability to evaluate and select information sources and digital tools based on the appropriateness to specific tasks
- Ability to recognize and authenticate sources and information online
 - Knowledge of how to locate, organize, analyze, evaluate, synthesize, and ethically use information from a variety of sources and media
 - Ability to judge the validity of content found on the Internet, know how/where to find appropriate material, and determine what sources can be trusted
- Understands what apps are and how they can be used to achieve/complete goals and tasks
- Understands the difference between hardware and software and how they work together
- Understands what is considered data and where to appropriately store data

Module Content

Searching and processing

- Misinformation is not always shared maliciously
 - We're more likely to share things we feel strongly about, especially things we hope are true
- Misinformation can, however, be shared on purpose to further individual agendas
 - It is important to double check your sources when you are searching for information online

In-class activity #1

Walk-through a scenario where one individual watches a video online and has a discussion with another individual:

- **Character 1:** Did you see that cute tiktok of that dog eating a chocolate bar?
- **Character 2:** I did, but I am a little confused because I thought that chocolate can make dogs sick?
- **Character 1:** Well, this tiktok had over 1 million views and was shared 50,000 times. I don't think it would be this popular if it weren't true

Provide the corresponding explanation:

- Sometimes people share misinformation by accident – because they think something is true. Most of us have probably shared something we thought was real without checking. We're more likely to share things we feel strongly about, especially things we hope are true.
- But sometimes people can share misinformation on purpose, to further their own personal agenda. It is important to double check your sources when you are searching for information on the internet.

- How do I search for information online?
 - The type of search depends on what you are looking for and where you are looking
 - Keyword searching is an effective way to search for information online
 - E.g., dogs + chocolate
 - Google searching – has the power to process full questions
 - E.g., Can dogs eat chocolate?
- Google is going to direct you to thousands of websites

- The next step is determining what is reputable and be used as an accurate source of information

Authenticating information

- What is considered a reputable source?
 - A credible source is one that is written by someone who is an expert in their field and is free of errors and biases².
 - Some examples include:
 - **Organizational or Government websites** (e.g., Diabetes Canada, SaskHealth Authority)
 - **University / academic centres** (e.g., University of Saskatchewan)
 - **Reputable news outlets** (E.g., CNN, The Globe and Mail, National Post, The New York Times, etc.)

In-class activity #2

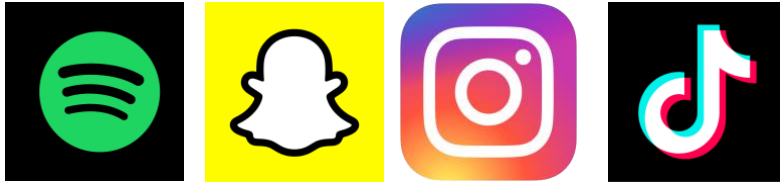
Provide either a screen recording, or demonstrate in-person, a search in Google looking for information (e.g., “Can dogs eat chocolate”). Filter through the search responses and identify which websites are reliable sources of information and which are unreliable.

- Scenarios where it is important to use reputable sources:
 - School papers
 - Medical information/research
 - News
 - Online shopping
- What is considered an unreliable source?
 - Unreliable sources can be written and altered by anyone and often include errors and biases².
 - Some examples include:
 - **Social media sites** (e.g., Facebook, Twitter)
 - **Wikipedia**
 - **Websites and blogs** with news that is based on opinion (e.g., Natural News)
- There are times when it's not necessary to use the most reliable sources you can find.
 - Examples include:
 - Recipes, DIY projects, background / basic understanding of a concept
- It is typically more important to verify sources rather than facts themselves
 - Two important questions to ask when verifying a source are:
 - Do they have a record of giving good information and correcting any mistakes?
 - Are they an expert (or qualified to discuss) on that topic?
- Indicators of a reputable source²:
 - Links to verifiable, current evidence
 - Use of language that is professional and clear of bias
 - Provide the author's name and information
- Comparing and synthesizing information from multiple sources
 - Looking at multiple sources can help you determine if the first source might have been misleading

- This is also a good way of discovering any possible bias that might exist in any one source

Apps

- Application (Apps)



- An app is a program, or a collection of programs that performs a specific task³.
 - Apps can be designed towards educational, professional, or personal purposes.
 - Other apps include: Email (e.g., Gmail), weather (e.g., The Weather Network), and FaceTime
- Many different types of apps and options within each type
 - The app you choose to use will depend on the task and what you are trying to accomplish

Computing

- A website is a collection of documents or web pages through the internet that contain information, images, and other media relating to a given topic⁴

In-class activity #3:

Play a mix-and-match game. Have students identify which items are hardware and which items are software.

- Hardware is any physical component of a computer such as microchips and keyboards⁵



- Software is a set of instructions, data, or programmes that are used to control a computer and accomplish specific tasks. Simply put, software instructs a computer on how to operate⁶



- Software can be programmed and needs to be updated

Data

- What is data?
 - Data is information that has been converted into a format that allows it to be moved, processed, and stored quickly⁷
 - A few common examples of data in your everyday life include:
 - Online purchases, photos & videos, and files on your computer

Data Backups

In-class activity #4:

Walk-through a scenario where a student spilled a glass of water on their computer without having saved their school project.

Highlight the importance of regularly saving documents and backing up devices.

- Backing up your data
 - Backing up your data, whether it is on your computer or phone, protects you from losing important information (e.g., draft of your school project, childhood photos)
 - There are multiple places where you can back up your data
 - Backing up a windows-based computer
 - Backing up an Apple device
 - Backing up an Android device
 - Backing up devices using Dropbox

Data storage

- Data is typically stored on servers
 - There are different types of servers⁸
 1. Local servers (E.g., computer, external hard drive)
 - Servers that you buy and own physical
 2. Clouds (E.g., icloud, google drive)
 - Servers you access remotely using the internet
 - A cluster of servers that work together as a single huge computing resource⁸
- How to decide where to store information⁹?
 - Local Servers:
 - Faster upload/download speeds
 - Higher security
 - Expensive & require maintenance
 - Cannot increase storage space
 - Can be physically damaged
 - Cloud servers:
 - Can be upgraded (software, storage space)
 - Can be access from anywhere
 - Requires internet access
 - Automatically backs up

Digital security & privacy

Learning outcomes

- Understands the concept of privacy in their everyday lives, and as it relates to using the Internet
 - Understands how to stay safe online by choosing websites that are safe and secure
- Awareness that many websites ask for information that is private and has the ability to responsibly handle such requests
- Knowledge how to identify secure sites by looking for privacy policies
- Knowledge of how and where to appropriately back up information
- Understands the reasons why people use passwords, the benefits of using passwords, and knows strategies for creating and keeping strong, secure passwords
- Understands data collection techniques
- Knowledge of digital worms/viruses and strategies to avoid them
- Knows strategies for guarding against identity theft and scams that try to access his/her private information online.

Module Content

Data Sovereignty

- Data sovereignty refers to meaningful control or ownership of one's data.¹⁰ It includes an individual's or community's "recognized right and legitimacy to exercise authority over its affairs"¹¹
- Data sovereignty includes having ownership and control of your personal data, as well as information about your community, such as resources or the environment (e.g., land history, geological information), data about your community's demographics or social data (e.g., legal, health, education), as well as cultural information (e.g., beliefs ancestral knowledge, community stories)¹²
- Data sovereignty is connected to self-governance. As described by Nikolakis (2019)¹³, "sovereignty and self-governance have different yet interdependent meanings in theory and practice. Sovereignty is a social, legal and political construct – the term conveys absolute power over people, land, water, and natural resources. Self-governance is an arrangement where a collective governs its own affairs, as a unit or subunit of sovereign power".¹⁴
- Animikii Inc.¹⁵ published a "Decolonizing Digital" series to examine how data and technology can be used to ensure data sovereignty for all Indigenous Peoples
 - Contextualizing Indigenous Data Sovereignty
 - Empowering Indigeneity Through Data Sovereignty
 - Data's Role in Indigenous Data Sovereignty
 - The Future is Indigenous
 - Our Data is Our Right
 - Developing Indigenous Digital Innovation
- The First Nations Principles of OCAP¹⁶
<https://youtu.be/y32aUFVfCM0>

In-class activity #5:

Discussion with students:

What does data sovereignty mean to you?

Why is data sovereignty important?

How do you think data sovereignty is connected to our self-governance? *

*For older students grade 7 and above the discussion can be expanded to discuss self-governance and other more complex topics. For younger students, discussion can be centred around data sovereignty and how it relates to their rights.

For a primarily non-indigenous audience, Animikii Inc.¹⁵ developed questions to help give context to this concept:

If your parents control your finances and only dole out payments via weekly allowances, do you have real authority over your own affairs?

If your parents are second-guessing everything you do, who's governing your behaviour?

If your parents meddle in your personal business and sow discord in your relationships, are they sticking their noses where they don't belong?

Now replace "your parents" with "the Government of Canada" and "you" with "Indigenous Peoples".

If the Government of Canada controls Indigenous Peoples' finances and only doles out payments via allowances, do Indigenous Peoples have real authority over their own affairs?

If the Government of Canada is second guessing everything Indigenous Peoples do, who's governing their behaviour?

If the Government of Canada meddles in Indigenous Peoples' personal business and sows discord in Indigenous Peoples' relationships, is the Federal Government sticking its nose where it doesn't belong?

- In order to enable our data sovereignty, what are key things we need to be aware of?
 - Data sharing
 - Privacy & security
 - Data collection

Data Sharing

- What is personally identifiable information (PII)?
 - Any factual or subjective information that can be used to identify an individual¹⁷
 - Examples: name, age, income, social security number, telephone number, etc.

Information	PII?
Name	No

Birth date	Yes
Age	No
Social insurance number	Yes
Credit card / bank information	Yes
Drivers license information	Yes
Names of pets	No
Hobbies	No

- Some online databases and systems will protect your personally identifiable information
 - Examples: research studies, census, bank systems
- There are some websites and databases, however, that do not have systems in place to protect your personal information
- It is important to understand why companies ask for personal information and how they intend to use it
 - This will help you decide who you can trust with your information and how much information you are comfortable sharing
 - If you aren't comfortable sharing information with the company, you may want to reconsider using their service

There are several ways to determine if a website/company will safely manage your data

- Questions to ask yourself when evaluating websites include:
 - Is this an organization you know and trust?
 - Have you read the terms and services?
 - Where is my data being stored?
 - Who has access to my data?
- Steps to help make an informed decision regarding sharing personal information online¹⁸
 - Contact person: Is there somebody I can contact if I have questions about the organization's privacy practices?
 - Collection: What personal information is being collected about me (e.g., name, credit card number, location)?
 - Use: How will the personal information be used (e.g., payment processing, identity verification, marketing, analytics)?
 - Disclosure: To whom will the information be disclosed (e.g., to a cloud computing company for storage)
 - Retention: Has the organization indicated that it has security measures or procedures in place to protect the information?
 - Access: How can I access the personal information the company has about me, and update it or correct mistakes if I find any?

In-class activity #6:

Provide either a screen recording, or demonstrate in-person, searching for a website in Google. Examine the website and discuss data storage practices outlined on the website.

Cookies

- Cookies¹⁹
 - Cookies are small files passed from a website to your computer, often without your knowledge
 - Cookies are used to save information (e.g., login details, preferences) about your web habits and build detailed personal profiles about you
 - The default is for websites to store all cookies indefinitely, with privacy options often being hard to find and modify
 - Clearing cookies:
 - Even though web browsers (e.g., google chrome, safari) can be set to block cookies, many websites require that you allow cookies to use their services
 - If you do block cookies, this often only clears traditional cookies but leaves super cookies or flash cookies
 - Blocking third-party cookies can impair the experience of some services, so users often must allow some cookies and not others
 - To clear all forms of cookies and web storage special add-on applications are required

Privacy & Security

- What is the difference between security & privacy?
 - **Security** refers to the protection of computer systems and networks against data leakage, theft, or damage to the electronic data, as well as distortion of services²⁰
 - The right to have some control over how your personal information is gathered and used is defined as the level of **privacy** protection that an individual has while connected to the Internet²¹

Passwords

Passwords are one way to keep your information safe²²

- There are two main rules of passwords:
 1. It must be strong
 2. Don't give it away
- What's considered a strong password?
 1. 8 to 12 characters
 2. Combination of lower and uppercase letters, symbols, and numbers
 3. One that's not reused for multiple accounts
 4. Doesn't include personal information (e.g., names of family members/pets/streets, or your birthday)

Digital Viruses

Clicking spam links could result in your data/computer being hacked or downloading a virus

- **A computer virus** (or malware) is a piece of harmful software or code designed to alter the way a computer operates and spread from one computer to another²³

- By modifying or destroying data, a virus might have unintended or detrimental consequences
- Several types of viruses exist (e.g., ransomware, botnets, trojans, worms)
- What to do if you download a virus:
 - If your device has not yet been compromised:
 - Delete the email
 - Immediately change your email password and any other passwords that may have been hacked
 - If your device has been compromised:
 - Contact a trusted IT professional
 - Additional information can be found here: <https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/phishing/>
- How to prevent against viruses/malware:
 - **Antivirus software** scans for, detects, and removes viruses from computers, as a means of protection²⁴
 - Most antivirus software operates automatically once installed, providing real-time protection against virus attacks¹⁶
 - Apple products have antivirus software built into their MacOS operating systems²⁵

Identity Theft

- Identity theft – what it is and how can I prevent it? ²⁶
 - When someone steals another person's personal information, usually for fraudulent motives, it is called identity theft
 - Examples of identity theft include: use of stolen credit cards, emptying your bank accounts
- Protection against identity theft looks similar to protection against viruses and scams²⁶:
 - Limit the personal information you share online, particularly sensitive information including your birth date and your social insurance number (SIN)
 - Do not share your banking information online or over email. If you need to share your banking information, do so over the phone or in person to people you trust
 - Carry only essential ID (e.g., driver's licence, health card) in your wallet. Leave your passport and SIN card at home
 - Passwords protect your information
 - Wipe your devices before disposing of them

Data Collection

- Why is data collected?
 - Data is collected in a variety of different ways for a variety of different purposes
 - We collect information every day (e.g., consulting friends, online searches) that allows us to make informed decisions (e.g., what to feed your dog, how to build a birdhouse)
 - At a higher level, data is collected (e.g., research studies, census) to facilitate important healthcare decisions, community program planning, and policy writing
- How is data collected?
 - Data is collected differently depending on the purpose
 - Informal data collection methods (e.g., consulting friends) can be used for everyday nonessential decisions

- Formal data collection techniques (e.g., research data collection) should be used for decisions and projects that have population-level implications

Ethics & Empathy

Learning outcomes

- Understands the concepts of ethical behaviour and online ethics
- Understands their responsibility to protect the privacy of themselves and others when sharing information online
- Understands that the information they put online leaves a digital footprint
- Understands what cyberbullying means and what they can do when they encounter it
- Understands the concept of having ownership over creative work and respecting the creative work of others
- Understands the importance of citing all sources when they do research
- Understands the concept of plagiarism, and when and how it is okay to use the work of others

Module Content

Digital Identity

- **A digital identity** is the publicly available online information about an individual, a company, or a piece of technology²⁷
 - In other words, it is a collection of information on someone found online
- It is important to remember that everything posted online leaves a **digital footprint**²⁷
 - The traces of your personal and professional information that are left in online networks - both intentionally and unintentionally
- The way you conduct yourself online should mirror how you conduct yourself in person. Before you share an opinion or information online, consider...
 - Would you say this to a friend?
 - Would you be embarrassed if someone said this to you?
 - Could this be taken the wrong way?
 - Could look bad to a university / college or a future employer?

In-class activity #7:

Historically Indigenous communities in Canada have been exploited when it comes to their personal information and data. This is an opportunity to stimulate discussion around maintaining privacy and strategies that are within their control specific community and heritage. Topics to consider include digital identity and footprint.

Digital Awareness

The 3 Rs of Digital Citizenship (Be social.Be smart blog)²⁸:

- **Be Responsible**
 - Use privacy settings thoughtfully and proactively
 - Know your friends and followers and be selective
 - Report inappropriate online behaviour and block haters or trolls
 - Assess the credibility and accuracy of online sources
- **Be Respectful**
 - Use your own voice and credit the originators of content you share
 - Be discrete with confidential, sensitive, and private information of others
 - Unplug in real social settings and nurture well-being with time offline

- **Be Reputable**

- Share digital content that reflects your values, interests, talents, and skills
- Build networks and engage with people who you can learn from
- Contribute to social change and community initiatives you believe in

Copyright & Plagiarism

- Plagiarism and copyright, what's the difference?
 - **Copyright** refers to the sole legal right to create, publish, or perform an original literary or musical work. It's used to secure original works of authorship as soon as they're published²⁹
 - **Plagiarism** is when you present someone else's work as your own, with or without their permission, and incorporate it into your work without giving them full credit³⁰
- Access to the internet has increased our exposure to other people's creative and intellectual property. It has also increased our ability to borrow and adapt someone else's work
- Copying of any sort can have consequences when posted online
 - Academic implications (e.g., failing a course, being placed on academic probation, or kicked out of college)
 - Legal implications (e.g., civil lawsuit)
 - Personal implications (e.g., loss of trust of a friend)

Harassment & Cyberbullying

- Consider what you should post about yourself... But also, what you should post about others
- **Cyberbullying** is any form of bullying that is done using technology. This can include sending hurtful text messages, sending embarrassing or inappropriate photos or videos, and spreading rumors about you online³¹
- Did you know?
 - 20% of teenagers in Canada report being the target of cyberbullying³²
 - 17% of teenagers in Canada report being a cyberbully at some point in their life³²
- Cyberbullying is becoming more common, and standing by without stopping it is part of the problem
- What to do if you witness cyberbullying?
 - Defending behaviour (i.e., attempting to stop bullying and provide comfort and support to victimized peers) helps reduce bullying in schools and has a protective effect on victimized peers³³
- What to do if you are being cyberbullied³⁴?
 - Most social networking sites have a policy for dealing with inaccurate or derogatory posts
 - Have a look for their procedure for complaining about a post or asking for something to be removed
 - Try contacting the website administrator with your concerns
 - Sometimes it is helpful to discuss the issue directly with the individual who made the post
 - If you feel threatened or harassed, seek advice from someone you trust or contact the police
- How can you prevent cyberbullying³⁵?
 - Make it clear to your friends that you won't be involved in bullying behaviour
 - Never stand by and watch or encourage bullying behaviour

- Do not harass, tease, or spread gossip about others, this includes on social networking
- Report it to someone in authority or someone you trust (e.g., at school to a teacher, or a school counsellor)

Consumer Awareness

Learning outcomes

- Knowledge of online spam, the forms it can take, and how to identify strategies for dealing with it
- Reading and understanding the implications of website Terms of Service and privacy policies
- Understands that the purpose of product websites is to encourage buying the product and is aware of methods used to promote products on these sites
- Understands the ways websites and companies collect data online and utilize it to personalize content for their users, as well as consider companies' motives in doing so

Module Content

Phishing

- **Spam** is the fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity in an electronic communication³³
 - Different types of spams exist: Phishing, spear phishing, etc.
- **Phishing** is an email scam that lures you under false pretenses to websites that look legitimate (e.g., banks, or disaster relief organizations) to get you to provide personal information³⁵
 - Be wary of anyone who asks for your bank or credit card details via email and only use secure sites when shopping online
 - Consider using a primary email address for your trusted contacts and creating a second email for your online activities (e.g., filling out forms or joining communities)
 - Ways to identify an email scam
 - Spelling mistakes
 - Uncommon email addresses
 - Email addresses from well-known companies with additional numbers and/or letters (e.g., no-reply.kgeiwqtpva@email.apple.com)

Terms of Service

- Terms of service / terms and conditions / terms of use
 - Terms and conditions are legal papers that guarantee that both the user and the provider are aware of their contractual rights and obligations. This is done in compliance with contract rules that govern contractual relationships at the municipal, state, and federal levels³⁶
 - It is very common not to read or skim the terms of service
 - These are a few things you should look out for:
 - Copyright, license
 - These terms often indicate that when you share data (e.g., personal information or photos) with this website, they can use it in advertising, sell it to a stock photo company, or release it to the media
 - Tracking, cookies

- These terms often indicate that websites compile large files on each of their users (and sometimes non-users) to serve you personalized advertisements
- Third-party, disclosure, partners
 - These terms often indicate that this website likely sells or shares your data to partner companies
- Monitor and customize your app permissions³³
 - During installation, you can adjust which permissions you give to each application
 - Consider what the app is used for, and which permissions would enhance your experience without compromising your privacy and/or safety
 - Common permissions include access to your **location, camera, and microphone**
 - Sometimes sharing this information is vital to the app's functionality, for example sharing your location with Google Maps in order to provide directions. However, Google Maps should not require access to your camera or microphone to provide directions.
 - You can view and modify your app permissions through your device settings or preferences
 - It is helpful to set permissions you don't mind sharing with a given app to "only when using". This will prevent the app from collecting this data when you are not actively using the application

In-class activity #8:

Provide either a screen recording, or demonstrate in-person, searching through an app's terms of service and permissions. Discuss which permissions are important for the app's functioning and which can be turned off. Discuss what the terms of service mean for data privacy and storage.

Digital Advertising

- Digital Advertising
 - There are different forms of digital advertising³³
 - Displaying the same advertisements to everyone visiting a particular website
 - Online behavioural advertising which shows you ads based on your personal browsing patterns
 - The online behavioural advertising approach aims to tell you about products or services you are likely to be interested in
- Have you ever discussed a product with your friends/family, and the next day you are receiving advertisements for it?
 - Your phone has access to your GPS and can detect who you spend time with based on your locations. Using this information, you could receive targeted advertising related to your friends and family's online behaviour patterns³⁴

References

1. British Columbia Ministry of Education and Child Care [Internet]. Victoria: The Ministry of Education; c2022. Digital Literacy Framework [cited 2022 Aug 2];[about 1 screen]. Available from: <https://www2.gov.bc.ca/gov/content/education-training/k-12/teach/resources-for-teachers/digital-literacy#:~:text=The%20Ministry%20of%20Education%20and,create%20and%20commu%20with%20others%E2%80%9D>
2. Austin Peay State University. *"Reliable and Unreliable Sources"*. Academic Support Center Writing Lab. Oct 29 2012. Web.
3. Computer basics: Understanding applications [Internet]. GCFGlobal.org. Goodwill Community Foundation, Inc; [cited 2022Mar24]. Available from: <https://edu.gcfglobal.org/en/computerbasics/understanding-applications/1/>
4. Techopedia. What is a website? - definition from Techopedia [Internet]. Techopedia.com. Janalta Interactive ; 2020 [cited 2022Mar24]. Available from: <https://www.techopedia.com/definition/5411/website>
5. Encyclopedia of business and finance, 2nd ed [Internet]. Encyclopedia.com. Encyclopedia.com; 2022 [cited 2022Mar24]. Available from: <https://www.encyclopedia.com/social-sciences-and-law/economics-business-and-labor/businesses-and-occupations/hardware>
6. The Editors of Encyclopaedia. [Internet]. Encyclopædia Britannica. Encyclopædia Britannica, inc.; [cited 2022Mar22]. Available from: <https://www.britannica.com/technology/software>
7. Data Definition & meaning [Internet]. Merriam-Webster. Merriam-Webster; [cited 2022Mar24]. Available from: <https://www.merriam-webster.com/dictionary/data>
8. The Editors of Encyclopaedia.[Internet]. Encyclopædia Britannica. Encyclopædia Britannica, inc.; [cited 2022Mar24]. Available from: <https://www.britannica.com/technology/cloud-computing>
9. <https://www.microsoft.com/en-ca/microsoft-365/business-insights-ideas/resources/cloud-storage-vs-on-premises-servers>
10. Hummel P, Braun M, Tretter M, & Dabrock P. Data sovereignty: A review. *Big Data & Society*. 2021;8(1): 205395172098201. <https://doi.org/10.1177/2053951720982012>
11. The First Nations Information Governance Centre. 'First Nations Data Sovereignty in Canada'. 1 Jan. 2019 : 47 – 69.
12. University of Alberta. Edmonton: UofA; c2022. Indigenous Research Guide. 2022 May 16 [Cited 2022 Aug 2]. Available from: <https://guides.library.ualberta.ca/indigenous-research>
13. Nikolakis W, Pierre S. The evolution of indigenous self-governance in Canada. In: Nikolakis W, Cornell S, Nelson H, editors. *Reclaiming Indigenous Governance: Reflections and Insights from Australia, Canada, New Zealand, and the United States*. University of Arizona Press, 2019. p. 55–70. <http://www.jstor.org/stable/j.ctvqc6jwv.7>.
14. Pierre S. *Reclaiming Indigenous Governance: Reflections and Insights from Australia, Canada, New Zealand, and the United States*. University of Arizona Press, 2019. <http://www.jstor.org/stable/j.ctvqc6jwv>
15. Animikii Inc. *Decolonizing Digital: Contextualizing Indigenous Data Sovereignty*. June 7, 2019. <https://animikii.com/news/decolonizing-digital-contextualizing-indigenous-data-sovereignty>
16. The First Nations Information Governance Centre. *Understanding the First Nations Principles of OCAP™: Our Road Map to Information Governance* [Internet]. [place unknown]: FNIGC; 2014 July 22 [cited 2022 Aug 2]. Video: 6:51 min. Available from: <https://www.youtube.com/watch?v=y32aUFVfCM0>

17. United States Department of Labor. (n.d.). Guidance on the protection of personal identifiable information. Guidance on the Protection of Personal Identifiable Information. Retrieved from [https://www.dol.gov/general/ppii#:~:text=Personal%20Identifiable%20Information%20\(PII\)%20is,either%20direct%20or%20indirect%20means](https://www.dol.gov/general/ppii#:~:text=Personal%20Identifiable%20Information%20(PII)%20is,either%20direct%20or%20indirect%20means).
18. Office of the Privacy of Canada. (2017, March 2). What to consider when reading a privacy policy. Office of the Privacy Commissioner of Canada. Retrieved from https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/your-privacy-rightCommissionerts/02_05_d_71_pp/
19. Office of the Privacy Commissioner of Canada. (2011, May). *Web tracking with cookies*. Office of the Privacy Commissioner of Canada. Retrieved from https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/cookies/02_05_d_49/
20. *What is Internet Security?* McAfee. (n.d.). Retrieved from <https://www.mcafee.com/enterprise/en-ca/security-awareness/cybersecurity/what-is-internet-security.html>
21. Encyclopædia Britannica, inc. (n.d.). *Privacy and the internet*. Encyclopædia Britannica. Retrieved from <https://www.britannica.com/technology/Internet/Privacy-and-the-Internet>
22. Office of the Privacy Commissioner of Canada. (2018, March 19). *Tips for creating and managing your passwords*. Office of the Privacy Commissioner of Canada. Retrieved from https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/tips_pw/
23. Office of the Privacy Commissioner of Canada. (2021, November 29). *Proceed with caution: Avoid malicious software*. Office of the Privacy Commissioner of Canada. Retrieved from <https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/phishing/#h07>
24. *What is antivirus - definition, meaning & explanation*. Verizon Fios. (n.d.). Retrieved from <https://www.verizon.com/info/definitions/antivirus/>
25. *MacOS - security*. Apple. (n.d.). Retrieved from <https://www.apple.com/macOS/security/>
26. Office of the Privacy Commissioner of Canada. (2020, October 28). *Identity theft and you*. Office of the Privacy Commissioner of Canada. Retrieved from https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/
27. Sector, D. T. S. (2021, June 5). *Digital Trust Series: Part 1 : Digital Identity*. Digital credentials. Retrieved from <https://www.ic.gc.ca/eic/site/153.nsf/eng/00001.html>
28. *The 3 RS of Digital Citizenship – being responsible, respectful and reputable*. Be Social. Be Smart. (2015, September 25). Retrieved from <http://www.besocialbesmart.com.au/uncategorized/the-3-rs-of-digital-citizenship-being-responsible-respectful-and-reputable/>
29. Office, U. S. C. (n.d.). *What is copyright?* What is Copyright? | U.S. Copyright Office. Retrieved from <https://www.copyright.gov/what-is-copyright/>
30. *What is plagiarism?* Plagiarismorg RSS. (n.d.). Retrieved from <https://www.plagiarism.org/article/what-is-plagiarism>
31. *Cyberbullying: What is it and how to get help: Violence, harassment and Bullying fact sheet*. The Australian Human Rights Commission. (n.d.). Retrieved from <https://humanrights.gov.au/our-work/commission-general/cyberbullying-what-it-and-how-get-help-violence-harassment-and-bullying>
32. Patchin, J. W., & Hinduja, S. (2013). Cyberbullying research: 2013 update. Retrieved from: <http://cyberbullying.us/cyberbullying-research-2013-update/>
33. Office of the Privacy Commissioner of Canada. (2018, August 23). *Protecting your privacy online*. Office of the Privacy Commissioner of Canada. Retrieved from

- <https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/protecting-your-privacy-online/>
34. *What you can do to stop bullies - be a supportive bystander: Violence, harassment and Bullying fact sheet*. The Australian Human Rights Commission. (n.d.). Retrieved from <https://humanrights.gov.au/our-work/commission-general/what-you-can-do-stop-bullies-be-supportive-bystander-violence>
 35. Office of the Privacy Commissioner of Canada. (2015, April 27). *Top 10 tips to Protect your inbox, computer and Mobile device*. Office of the Privacy Commissioner of Canada. Retrieved from https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/spam/casl_tips_ind/
 36. *I read the terms of service, so that you don't have to*. The Mowat Centre. (n.d.). Retrieved from <https://munkschool.utoronto.ca/mowatcentre/i-read-the-terms-of-service-so-that-you-dont-have-to/>

Digital literacy - Baseline assessment

1. What gender do you identify as?

- A. Male
- B. Female
- C. Non-binary
- D. Other: _____
- E. Prefer not to answer

2. What is your age? ____

3. What grade are you in?

- A. Grade 9
- B. Grade 10
- C. Grade 11
- D. Grade 12
- E. Not applicable

4. How often do you use the internet?

- A. Several times per day
- B. Once a day
- C. A few times a week
- D. A few times a month

5. On average, how many hours a day do you spend on the internet?

- A. Less than an hour
- B. 1-3 hours
- C. 4-5 hours
- D. More than 5 hours a day

6. What do you like doing most on the internet? *Select all that apply.*

- A. Gaming
- B. Social media (e.g., Snapchat, Instagram, Facebook, Twitter, YouTube)
- C. Shopping (e.g., Amazon, UberEats)
- D. Web browsing
- E. Other: _____

7. Where do you usually have access to the internet?

- A. Full time access (anywhere)
- B. At home only
- C. At a public space (e.g., school, library)

8. How do you communicate with friends and family online?

- A. Email
- B. Video Call (e.g., Facetime, Skype, Zoom, What's App)
- C. Phone Call
- D. Messaging
- E. Other:_____

9. Which of the following social networking sites do you use? *Select all that apply.*

- A. Facebook
- B. Instagram
- C. Twitter
- D. Whatsapp
- E. Snapchat
- F. Other_____

10a. Do you read the terms and services when you install programs or apps?

- A. Yes, always
- B. Sometimes, depends on the app/program
- C. No, I just accept without reading
- D. I don't know

10b. Do you understand the terms and services when you install programs or apps? [If A or B is selected in question #10a]

- A. Yes
- B. No

11. Who has permission to see or use your online information ? For example, data about your behavior online, such as your photos or your location. *Select all that apply.*

- A. No one can access it
- B. I give permission to private companies to store and use my data (e.g., Facebook, Instagram, Google)
- C. I give permission to companies that I have heard of, and I trust (e.g., public, educational, or governmental organizations)
- D. Anyone who wishes, those data are not mine anymore
- E. I don't know

12. How much thought do you put into shaping your digital identity (i.e., the publicly available online information about an individual, a company, or a piece of technology)?¹

- A. A lot (e.g., I carefully choose which pieces of information or photos to share about myself)
- B. Some (i.e., I don't pay too much attention, I provide information of photos if I feel like it))
- C. None (I post and share information openly)
- D. Not applicable (I don't give any information online)

13. Which of the following statements apply to you? *Select all that apply.*

- A. I know how to recognize cyberbullying if I see it.
 B. I know how to address cyberbullying if I see it.
 C. I know how to prevent cyberbullying from happening.

14. Please indicate your level of agreement with the following statements:

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I know how to...					
Protect my privacy and safety in online communities					
Selecting and install an app on my mobile device(s)					
Use mobile tools (e.g., text, email, mobile learning management systems (Microsoft Teams), social networks) for school-related activities					
Check for accuracy and authenticity when searching for information on the Internet					
Create/change my password					
Back up my data (e.g., photos, files) onto a server					

15. Please indicate your level of confidence completing the following tasks:

	Not at all confident	Neutral	Somewhat confident	Very confident

Solving my own technical mobile-related problems				
Protecting my mobile device(s) from spam and viruses				
Using mobile maps to navigate around				
Searching and evaluating information using mobile devices				

References:

1. Sector DTS. Digital Trust Series: Part 1 : Digital Identity. Digital credentials. 2021, June 5.

Retrieved from <https://www.ic.gc.ca/eic/site/153.nsf/eng/00001.html>