Privacy Pursuit!
The Value of Privacy

Grades: 6–7

Teacher's version

Framework Topics:
Privacy and Security,
Consumer Awareness

Duration:
1 to 1½ hours

Overview:
In this lesson, students learn how their personal information is key to how most of the "free" apps and platforms they use make money. They learn practical strategies and tools for managing their privacy and plan how these can be used to limit what audiences have access to their personal information.

Share your thoughts on this lesson with us!

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

This lesson was created by MediaSmarts for the Information and Privacy Commissioner of Ontario.

MediaSmarts
Canada's Centre for Digital Media Literacy

Learning Outcomes

Students will understand the following key concepts/big ideas:

Media have commercial considerations

- Media works such as apps and websites that seem to be free are usually paid for with your attention, your personal information, or both

Digital media are are networked

- Information on a connected network can reach any part of that network

Digital media are shareable and persistent

- Once you post something, it can stay online or be shared forever and can be copied, altered, and used in ways you don't like

Digital media have unanticipated audiences

- Things you post online — and information collected about you — may be seen by people you didn't expect and may not even know about

Students will learn the following essential domain knowledge:

Privacy and Security

- Privacy risks include scams, embarrassment, hurting people's feelings, cyberbullying, and threats to property or personal safety
- Taking proactive steps to manage your privacy can limit privacy risks
- Be careful what personal information you share online
- Privacy settings can control who sees what you post
- Passwords are an important tool to protect your privacy
- Some websites, apps, and services should be previewed by trusted adults, or not used by children at all
- Create pseudonymous usernames and avatars for online gaming
- Trusted adults are important resources for help-seeking before and after privacy risks occur
- Don't click on unknown links or download files from unknown senders

Consumer Awareness

- Most "free" apps make money from selling advertising, and in some cases by collecting and selling personal information
- Advertisers will pay more if ads are targeted to you using your personal information
- Platforms also use your personal information to show or recommend content that will keep you interested and viewing ads

Students will learn how to:

- Use: Manage privacy risks by proactively employing privacy strategies
- Understand: Analyze the privacy risks of different devices, apps and online activities
- Engage: Develop strategies for limiting the impact of data collection on their online experience

Personal Data Protection Competencies

Personal Data

- I understand what is involved in the concept of personal data, defined as any data — whether or not it was made public — about an identifiable individual
- I know and understand the concept of pseudonymity and masking one's identity
- I can give examples of personal data that can directly identify individuals (civil/family status, photo of a student in the class, etc.) and technical data that can monitor the activities of a person and identify them (cookies, geolocation data, etc.)

Understanding the Digital Environment

- I know what the internet and its services are (social networks, mobile applications, the cloud, etc.)
- I know the key IT risks; I know digital security is important and understand the need to ensure the physical and logical security of a digital environment
- I am careful to only share the personal data that is absolutely necessary to register for a service
- I know that there are ways to protect myself online
- I assess my practices and develop problem-solving and learning reflexes — namely about security — by identifying resources (user communities and forums, tutorials, etc.)
- I know who the key player groups in the digital economy are (e.g., ISPs, service providers, developers, curators, etc.)
- I understand the systems used to market products and offer free services (loyalty cards, targeted advertising via cookies, setting up user accounts, subscribing to newsletters, etc.), for the purpose of establishing personalized user profiles
- I can give examples of digital services whose economic model involves — or does not involve — the collection of personal data

Managing My Data

- I know that I can manage the settings of the online applications and services that I use
- I know that, to use certain online services, my consent or consent of my parents/legal guardians is required
- I use procedures available to protect my personal data

Preparation and Materials

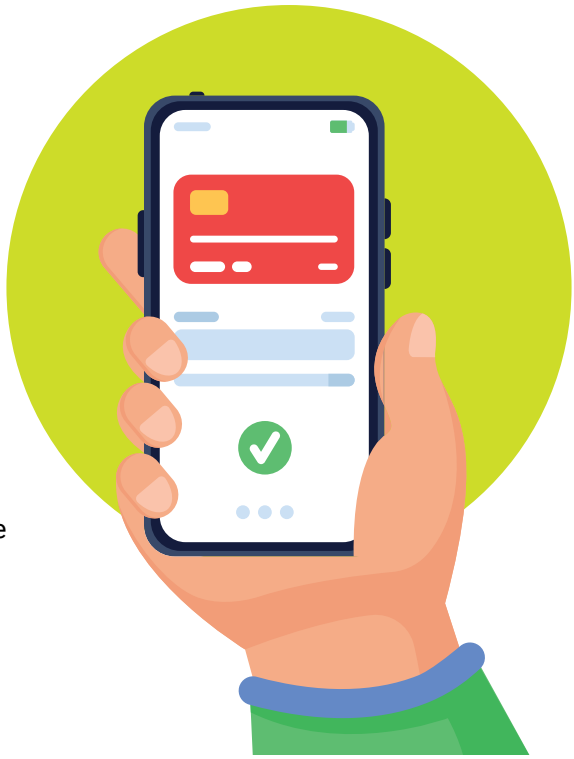
Prepare to distribute either the full *Privacy Pursuit!* booklet or the following pages:

- Page 2: Have Fun Learning About Online Privacy
- Page 6: Why Worry About Privacy… What Can Happen?
- Page 9: 11 Great Ways to Protect Privacy

Prepare to distribute the handout *Audiences.*

Procedure

How are You Paying?



Start by having students draw up two columns on a piece of paper. Have them list all of the *paid* apps (ones that you pay to purchase, that have a subscription fee, or that include in-app purchases) that they use in the left-hand column, and all of the *free* apps (that you do not pay money for in any way) in the right-hand column. (If they do not know whether an app is paid or not, have them put it in the free column.)

Now ask students: Which list is longer? Have students name some of the free apps that were included in the right-hand column and list them on the board. They will likely include social networks such as Instagram and Snapchat.

Ask students: If these apps are free, how do you think they make money? Let students suggest a few answers without indicating whether they are right or wrong.

Distribute or display the box titled "Did You Know?" on page three of the *Privacy Pursuit!* booklet and have students read it. Point out that a small number of apps and platforms, like Scratch and Wikipedia, really are completely free, but for most apps that seem free, you actually pay with your attention, by watching ads.

Now ask: How is your *personal information* part of how they make money? Pause to review the definition of *personal information* (anything that can identify you.) Let students discuss the question and make sure they understand the following points:

- Most free apps make money by selling ads
- Advertisers believe these ads are more valuable because the apps use what they know about you (your personal information) to target you with ads that will appeal to you
- Many apps, including social networks like Instagram and video sites like YouTube, also use your personal information to decide what to *show or recommend* to you. This keeps you on the site longer so that you see more ads.

Privacy Risks

Distribute or display page six, "Why Worry About Privacy… What Can Happen?" and have students read it.

Have students plot the different risks on a graph by how likely they are to happen and how serious they would be if they did happen. Have students share how they graphed different risks and discuss as a class: Which should we worry about the most?

Optional: If you feel your students need a better understanding of the concept, show them the *Digital Literacy 101* video ***Digital Media Have Unexpected Audiences***.

Taking Control

Distribute or display page nine, "11 Great Ways to Protect Privacy." Read through strategies with the students and discuss which of the risks you've just discussed each strategy would address.

Assessment

Distribute the handout *Audiences*. Have students choose an app or platform they use or know of and list, in the rings around the central image, the different possible audiences:

- In the centre ring, people you want to see the content
- In the second ring, people you don't want to see the content, but who might see it anyway
- In the third ring, people who might see the content without you knowing it or who might see it sometime in the future

Prompt students to consider more than just social networking or messaging apps. Point out that any app, game, or tool that lets you communicate with other people — including video games with chat functions or ones that let you post content like Scratch — allow different audiences to see what you share.

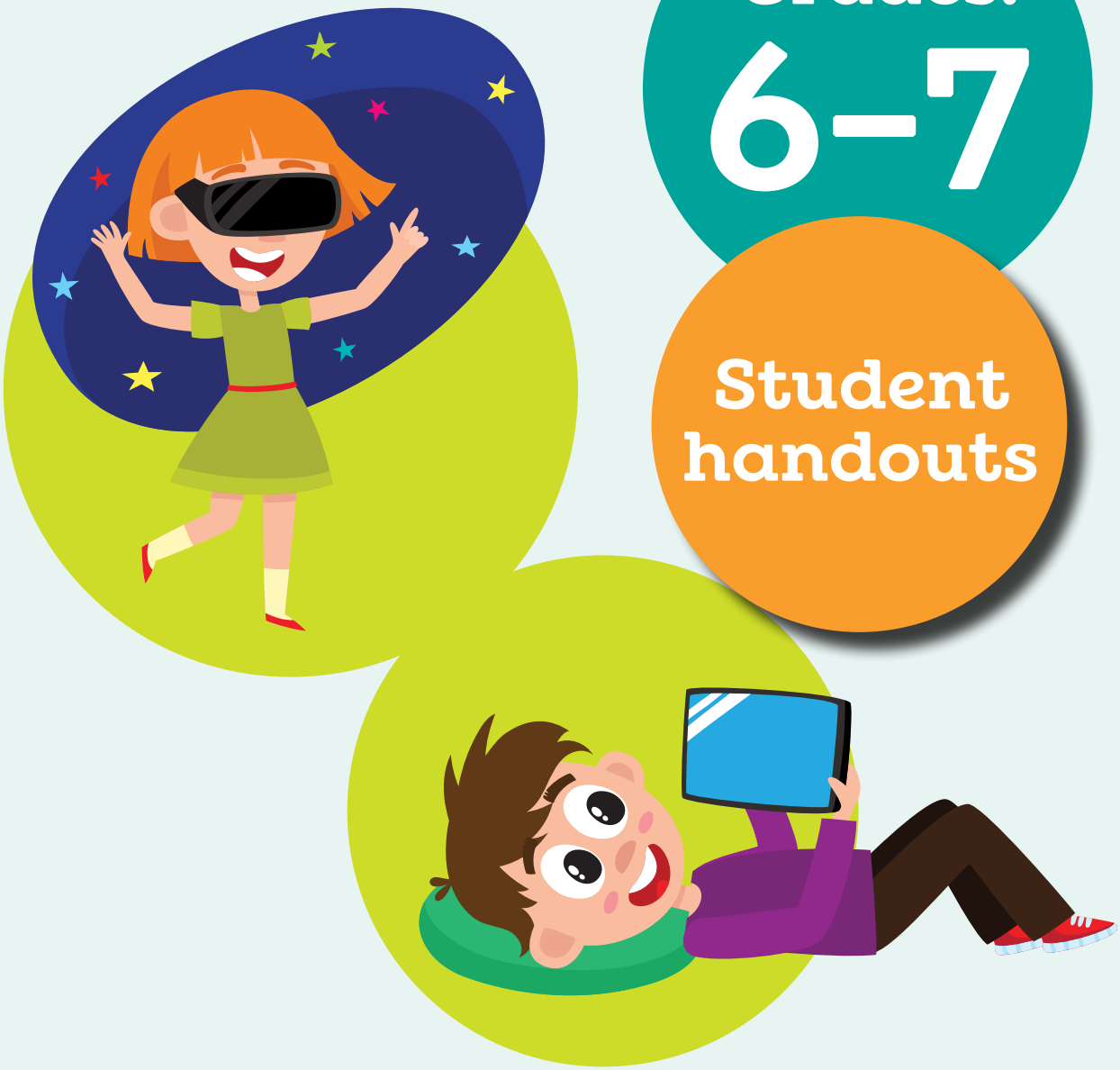
Then, have students list on the other side of the page different strategies (from the list on page nine) that would prevent or limit each of these audiences from seeing what they post or share.

Privacy Pursuit!

The Value of Privacy

Grades: 6–7

Student handouts



Share your thoughts on this lesson with us!

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

This lesson was created by MediaSmarts for the Information and Privacy Commissioner of Ontario.

MediaSmarts
Canada's Centre for Digital Media Literacy

Audiences

In each of the squares below, list the people who *might* see something you post online.

In the smallest box, list the people you *want* to see it. In the middle box, list the people who *might* see it if people in the first box share it. In the biggest box, list the people who might see what you post without you knowing it.

Unknown audiences

Unwanted audiences

Intended audiences

Controlling Audiences

Now that you've thought of some of the different audiences that might see what you post, name which *privacy strategies* would make it harder for each of them to see what you post or share. You can use strategies from the list in "11 Great Ways to Protect Privacy," but you can add your own too!

Intended Audiences: What strategies can you use to make sure just *some* of the people you're connected to online see something that you're posting?

Unwanted Audiences: What strategies can you use to make sure what you've posted *isn't* seen by the people who weren't meant to see it?

Unknown Audiences: What strategies can you use to stop people (or companies) you don't know from seeing what you see and do online?