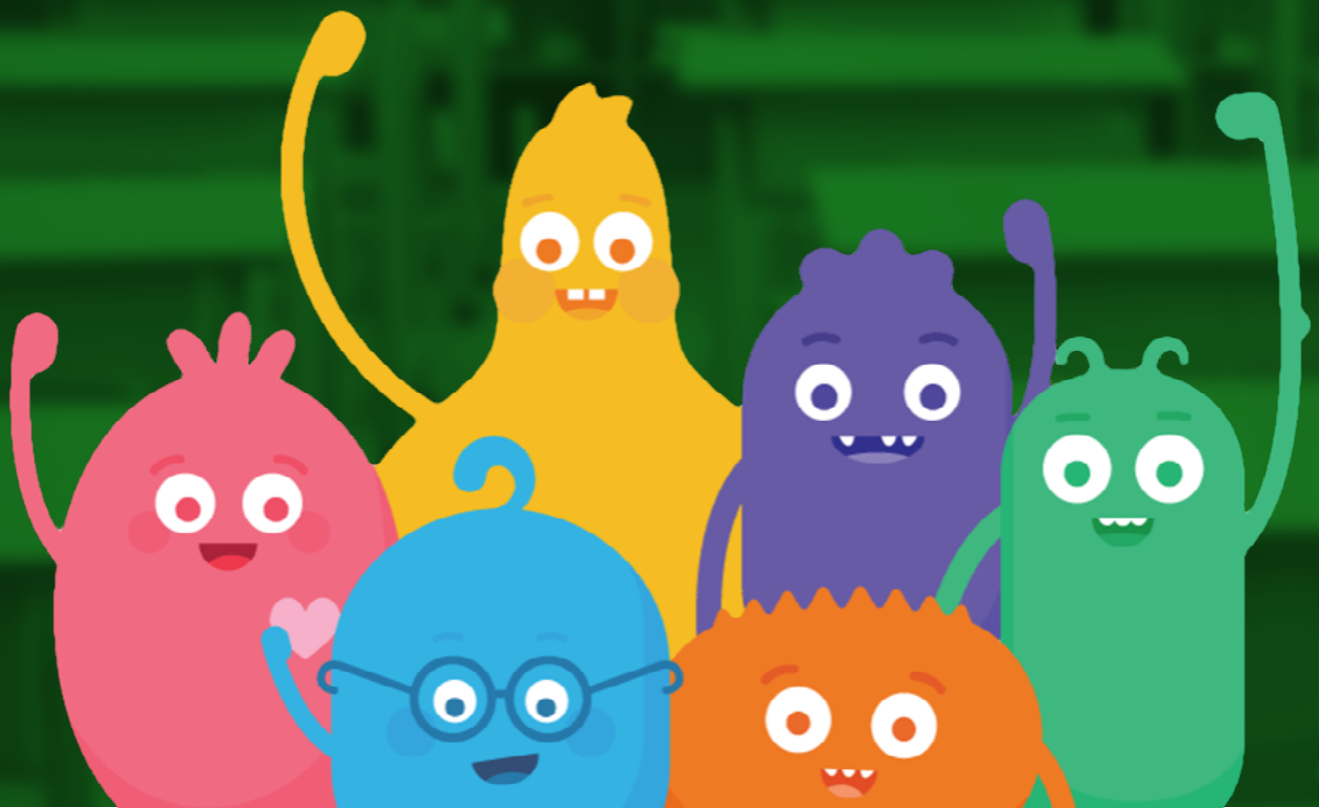
GRADE 8

K-12 Digital Citizenship

POWERED BY common sense education®



INFOSEC

Grade 8: Program plan

GRADE	TIME	TOPICS
8	50 mins.	• Privacy & Security • Digital Citizenship

Being Aware of What You Share

How can you protect your privacy when you're online?

Kids share a lot of information whenever they go online -- sometimes on purpose, sometimes not. But do they understand that online privacy isn't just what they say and post? Help your students learn about their digital footprints and the steps they can take to shape what others find and see about them.

Students will be able to:

- Reflect on the concept of privacy, including what they feel comfortable sharing and with which people.
- Analyze different ways that advertisers collect information about users to send them targeted ads.
- Identify strategies for protecting their privacy, including opting out of specific features and analyzing app or website privacy policies.

Key Standards Supported

COMMON CORE

L.8.1, L.8.2, L.8.2c, L.8.3, L.8.4, L.8.6, RI.8.1, RI.8.2, RI.8.4, RI.8.10, SL.8.1, SL.8.1a, SL.8.1b, SL.8.1c, SL.8.1d, SL.8.2, SL.8.3, SL.8.4, SL.8.6, W.8.4, W.8.10

CASEL

1a, 1b, 1c, 1d, 1e, 2a, 2b, 2c, 2d, 2e, 2f, 3a, 4a, 4b, 4c, 4d, 5a, 5b, 5c, 5d, 5e, 5f

AASL

I.A.1, I.A.2, I.B.1, I.B.2, I.B.3, I.C.1, I.D.1, I.D.2, I.D.3, I.D.4, II.A.1, II.A.2, II.B.1, II.B.2, II.B.3, II.C.1, II.C.2, II.D.1, II.D.2, II.D.3, III.A.1, III.A.2, III.B.1, III.B.2, III.C.1, III.C.2, III.D.1, III.D.2, IV.B.2, IV.B.4, V.A.2, V.A.3, V.C.1, V.C.3, V.D.1, V.D.2, VI.A.1, VI.A.2, VI.A.3, VI.D.1, VI.D.2, VI.D.3

ISTE

2a, 2b, 2d

What You'll Need

Some resources below are available in Spanish

IN CLASS

- Lesson Slides
- Ad Detective
  Handout
  Teacher Version
- Lesson Quiz

FOR FAMILIES

- Family Activity
- Family Tips
- Family Engagement Resources

Lesson Plan

Warm Up: **Private Minds** 10 mins.

Before the lesson: As an optional activity before the lesson, have students complete the **Sticky Situation** storyline in **Digital Compass™** by Common Sense Education. This will help introduce key concepts of this lesson. To see more, check out the **Digital Compass Educator Guide**.

1. **Project Slide 4** and ask: *What do you think of this meme? Do you think it's funny?* Call on students to share. Point out and confirm that the bottom image shows someone's reaction to learning that their mind was being read!

2. **Say**: *Even though mind reading might seem like a really cool power for someone to have, it actually would be pretty scary for everyone else. We all have thoughts that we don't intend or want others to know. These are our private thoughts, and we'd probably feel embarrassed or vulnerable if someone else knew them. Not sharing our private thoughts is an example of* ***privacy****, which is protection from being observed or tracked by others. This includes protection from other people as well as groups of people, like companies, the government, or the general public.* (**Slide 5**) *Legally, we all have certain rights related to privacy.*

3. **Ask**: *Can you think of examples of things that people might want to keep private -- either from everyone or from specific people?*

   Call on students to respond. If students are reluctant to share, provide examples:

   - *Not sharing your true thoughts because you don't want to hurt someone's feelings (maybe you secretly don't like Grandma's famous pumpkin pie!).*
   - *Not sharing with your parents certain things you talk about with your best friend.*
   - *Certain personal preferences you wouldn't want others to know.*

   Explain that people have different boundaries when it comes to what they share with others. Some people feel comfortable sharing a lot with others, while others don't share a lot with anyone, even their close family.

4. **Say**: *When you are online, privacy becomes more complicated. You can choose the websites you go to and what information you decide to share with others, like on social media. But, depending on the device, app, or website you're using, your words and actions are often being collected and tracked. Today, we're going to talk about how you can better understand what information is being collected and used about you online, particularly by companies.*

Explore: **Just for You** 10 mins.

1. **Say**: *We're going to begin by looking at a scenario.* Distribute the **Ad Detective Student Handout** and have a student read the scenario aloud. Ask: *What do you think about this scenario with Keet? How would you feel if this happened to you?*

   Call on students to respond. Follow up by asking if their feelings would change if the ads were for something besides shoes. Ask: *What if your best friend moved to another country and all of a sudden you started seeing ads for plane tickets to that country?* Students may say they're less comfortable with that because the ads aren't based on their shopping history but on something more personal.

2. **Say**: *Companies place ads online based on everything they know about you. It might be based on information you provided when you signed up. Or it might be based on something you searched for, looked at, liked, or posted while using the app. It's also based on information they get about how you use the app: how often you use it, what time of day, etc. The websites and apps you use -- and the devices you use them on -- can collect a lot of information about you. Companies then try to target you with ads or content that can appear in different places.*

3. **Direct** students to go back to their handouts and work in pairs to answer **Question 1**.

4. **Call** on students to share their responses. They may correctly identify that *when Keet went to the online store, it was likely tracked by the search engine and his device.* And *when he posted the link on social media, it was likely tracked by his social media app.*

   Next, let's dive deeper into how this all works and how you can protect your own privacy.

Analyze: **Protecting Your Privacy** 20 mins.

1. **Project Slide 6** and ask: *Has anyone seen a screen like this before? What is it?* Call on students to respond. Clarify that it is a sign-up screen for Snapchat, an app that many of them may know about. Follow up by asking: *When someone signs up for and uses Snapchat, what information do you think they are sharing? Who are they sharing it with?*

   Call on students to respond. Sample student responses:

   - information required during sign-up (*name, phone number, and birthday*)
   - "snaps" or content that the user creates, which might be shared with Snapchat or with friends of the user
   - things you browse when you're using the app
   - your location

   Confirm that all of those things get shared with Snapchat and that the first way to protect your information is to understand what companies are collecting about you. If there's something that students don't want companies or others to know about, they shouldn't provide or post it.

2. **Say**: *Companies get information about you by tracking what you do. One way they do this is by using **cookies**. A cookie is a small text file placed on your device by the sites you visit. It allows companies to collect information about you and what you do while you are on their site. Companies use this information to learn your preferences so they can make recommendations of things you'll like and make it easier for you to use their site, and they also may sell this information to advertisers and other companies.* (**Slide 7**)

   Ask: *In Keet's scenario, how might a cookie have helped advertisers figure out what he was interested in?*

   Call on students to respond. If necessary, clarify that when Keet went to the online store Zaps, they used cookies to track what he shopped for. That information was then shared with advertisers, who used it to place ads in the apps and websites that he uses.

3. **Project Slide 8** and say: *If you're not comfortable with this kind of tracking, you can turn cookies off in your browser settings. You can usually find the setting in the privacy settings. You should know that this might affect your browsing experience, as cookies also help the website automatically know helpful things about you, like your location or preferences.*

4. **Project Slide 9** and ask: *Let's talk about another tip for protecting your privacy. What do these screens show? What could you use them for?* Call on students to respond. They may correctly identify these screens as settings screens.

   Say: *Most apps have settings you can adjust, and these are screenshots of the settings screens in Snapchat. Within an app's settings, there are usually **privacy settings**, which are choices a website or app gives you about what information is visible to other users and third parties. You can usually use these settings to opt out of some of the ways that the app shows and shares your data. **Opting out** means choosing not to participate in something.* (**Slide 10**)

5. **Go** back to **Slide 9** and ask: *What might you click on in these screenshots to see or adjust your privacy settings?*

   Call on students to respond and support them to correctly identify the "WHO CAN … " section and review the items in it. Project **Slide 11** to confirm tips for protecting privacy.

6. **Project Slide 6** again and say: *Another way you can protect your privacy is by looking at what you're agreeing to when you sign up.* Direct students' attention to the fine print above the "Sign Up & Accept" button. Point out the two words in bold: "Privacy Policy" and "Terms of Service." Say: *These two terms are important! They actually tell you everything you're agreeing to, legally, when you agree to use the app. A* ***privacy policy*** *describes what user information the app or website collects and how they use it. The* ***terms of service*** *describe the rules that the company and users must obey when they use the app.* (**Slide 12**) *These documents are usually pretty long and sometimes difficult to understand. They are legal agreements users opt in to.*

7. **Say**: *Remember the word* ASK *when you're looking at a privacy policy.*

   Review the acronym ASK on **Slide 13** and explain that by finding out these pieces of information, students can make an informed decision about using the app or opt out of certain kinds of tracking.

Wrap Up: **Take Action** 10 mins.

1. **Project Slide 14** and review the final tip for protecting privacy. Ask: *Based on these tips, what do you think Keet could have done if he wanted to protect his privacy more? Go back to your handout and answer Question 2.*

   Call on students to share out their answers. Refer to the **Teacher Version**.

2. **Ask**: *What information are you OK with your devices, apps, and websites collecting? Does it depend?* Take turns sharing with your partner.

   Call on students to respond. Prompt students to identify specific pieces of information they're OK with sharing as well as information they're not OK with sharing. And ask them to consider whether the benefits and importance of the device, website, or app factors in to their thinking. (For instance, do they need their location tracked if the app doesn't depend on it to function?)

3. **Direct** students to complete Question 3 on their handouts. Collect handouts to assess student learning.

4. **Have** students complete the **Lesson Quiz**. Send home the **Family Activity** and **Family Tips**.

Additional Resources:

1. **Extend the lesson:** Reinforce the learning objectives from this lesson by having your students watch our **Digital Connections video series**. The videos address key digital citizenship topics like:

   - Practicing media balance
   - Being kind online
   - Staying safe when using tech
   - Identifying misinformation online

   There are six videos, and each includes reflection questions and a quiz. The series can be completed as a self-guided activity, as homework, or even as part of a future digital citizenship lesson.

2. **Extend the lesson:** Have students apply what they have learned by completing the **"Social Media Privacy" Activity** on TestDrive, a social media simulator. Students go through a self-guided activity to reinforce key concepts and practice managing privacy settings online. For more information, download the **Social Media TestDrive Educator Guide**.

3. **Extend the lesson:** Provide students with a link to a privacy policy, such as those for **Snapchat** or ***Fortnite***, and have them complete a Scavenger Hunt to find specific information such as:

   - what data the app or website collects
   - what data is collected from third parties
   - what data is shared with third parties
   - how long user data is stored

EXTEND THE LESSON

Common Sense Education has partnered with CYBER.ORG to support cybersecurity education. If you want to build on the themes from this lesson, we recommend the following lesson from the **CYBER.ORG content library**:

- **Layers of Protection for Your Internet Voyage (Grades 6–8):** Students will explore how combining good cybersecurity practices can increase user safety when exploring the internet.

Our collaboration with CYBER.ORG was made possible with the generous support of Craig Newmark Philanthropies.

© Common Sense Media. Lessons are shareable with attribution for noncommercial use only. No remixing permitted. View detailed license information at creativecommons.org.

Lesson last updated: August 2019