Teaching Privacy to Your Students

Objectives

- Understand the **need** to teach students about privacy.

- Recognize the myriad privacy **risks** students face online.

- Learn **privacy tips** for students and **key topics** to cover.

- Discover useful **lesson plans**, **activities**, and other **resources** to adapt for your classroom.

Why Teach Privacy?

- As students are finding more and more of their lives mediated through technology and online, this is a great opportunity to educate your students about [digital hygiene, safety, and privacy](#).

- Students should be aware of the **risks** and **opportunities** they will encounter online.

- Teachers should help students **understand** the online environment, help students **shape** their opinions on acceptable and unacceptable use of their personal information, and **empower** students to take control of their privacy,

Privacy Risks for Students

STUDENT PRIVACY COMPASS

Risk #1: The Internet is Forever

When a student posts something online, it will exist on the internet forever (even if they "delete" it). Students should be conscientious about the information they post about themselves online and assume that anything they put online could be accessed by anyone at any time.

Risk #2: Students are Prime Targets for Hacking and Identity Theft

Students are attractive targets for identity theft since they have clean credit histories. Be sure students never post their social security numbers online and view anyone who asks for it with suspicion. The impacts of identity theft can be far-reaching and extremely damaging.

Risk #3: Distance Learning Leaves Students More Exposed

Students participating in virtual classrooms can inadvertently reveal details about their lives they may not have chosen to share in the traditional school environment. Encourage alternative means of participation if students are concerned or uncomfortable using certain tools. Tell students to be mindful of what others can see during online class sessions and on online learning platforms. Urge students to speak up if they ever feel uncomfortable.

Guiding Questions for Students

1. **What** is privacy?

2. **Who** needs privacy and why?

3. Who should be allowed to **collect**, **access**, **use**, and **retain** our personal information?

4. Under what circumstances, if any, should someone be allowed to access our personal information **without our consent**?

5. If we share our own personal information with another person, government, company, or school **what should they be allowed to do with it**?

Key Topics for Students

- Types of **Personally Identifiable Information**
  - Activity Example: Common Sense Education, [Keep it Private!](#)

- Online **Terms of Service (ToS)** and **Privacy Policies**
  - Lesson Example: Common Sense Education, [Be Aware of What You Share](#)

- **Targeted Advertising**
  - Lesson Example: Teaching Privacy, [Information is Valuable](#)
  - Activity Example: Common Sense Education, [Ad Detective](#)

- **Geolocation Tracking**
  - Video Example: Fordham CLIP Privacy Educators Program, [Mobile, WiFi, and Facial Recognition](#)

- **Surveillance**
  - Electronic Frontier Foundation, Surveillance Self-Defense, [Privacy for Students](#)

Privacy Tips for Students I

STUDENT PRIVACY COMPASS

- **What you post can last a lifetime:** Before posting online, think about what others might learn about you and who might see it in the future – teachers, parents, colleges, and potential employers. Share the best of yourself online.

- **Be aware of what's being shared:** Be aware that when you post a picture or video online, you may also be sharing information about others or personal details about yourself like where you live, go to school, or hang out.

- **Post only about others as you would like to have them post about you:** The golden rule applies online as well. Ask permission before you tag a friend in a photo.

- **Own your online presence:** It's OK to limit who can see your information and what you share. Learn about and use privacy and security settings on your favorite online games, apps, and platforms.

- **Know what's being collected, who is collecting it and how it will be used:** Information about you, such as the games you like to play, what you search for online, and where you shop and live, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps and websites. Only use a product or service if the company is open and clearly states how it will use your personal information. If you're not sure what a business will do with your information, ask your parents.

Source: National Cybersecurity Alliance, Privacy Tips for Teens

Privacy Tips for Students II

STUDENT PRIVACY COMPASS

- **Use privacy settings:** Choose how your data is collected or shared by customizing your privacy settings. If a website, social media site, or app does not give you privacy setting options, you may want to consider not using that site or app if you want to protect your information.

- **Delete data:** When you find yourself no longer using a site or app, you can choose to delete your account or data.

- **Browse securely:** Make sure that the URL at the top of your browser includes the text "https://", rather than "http://," which means that the website secures the exchange of information on the site so when you share information, it is safer.

- **Use privacy-protective tools:** Download and use browser plug-ins like Disconnect or AdblockPlus that limit unwanted tracking and advertisements.

- **Go incognito:** Most browsers allow you to use a "private window," which means that your browser will not keep data about your browser history or cookies. This makes it more difficult for websites to track you and your information.

Activity

1. Consider the student privacy risks pre-COVID-19 in the **traditional school setting**.

2. Consider the student privacy risks post-COVID-19 with **remote learning**.

3. Which risks are the **same** and which are **different**?

4. Identify the **strategies** you as an **educator** can employ to **mitigate** the risks.

5. Identify the **strategies** your **students** can employ to **mitigate** the risks.

6. Create an **action plan** to teach students the privacy risk mitigation strategies you identified.

Resources

- ISTE's [Digital Citizenship](#) course for K-12 teachers
- Common Sense Media's [Digital Citizenship](#) lesson plans for K-12 teachers
- [Digital Citizenship+ Resource Platform](#), which includes lesson plans and activities
- [My Privacy UK](#), funded by the United Kingdom's privacy agency, with lessons, videos, and activities for children
- Canadian Civil Liberties Association's [Peer Privacy Protector Project (PPPP)](#), created for Canadian students, but useful and relevant information for American students as well
- Fordham CLIP's [Privacy Educators Program](#) includes lesson plans and visual aids for teachers
- International Computer Science Institute and the University of California-Berkeley's [Teaching Privacy Project](#)
- MIT Media Lab, [AI + Ethics Curriculum for Middle School](#)
- Google for Education's [Digital Citizenship and Safety](#) course for teachers and [Be Internet Awesome](#) lessons and activities for students