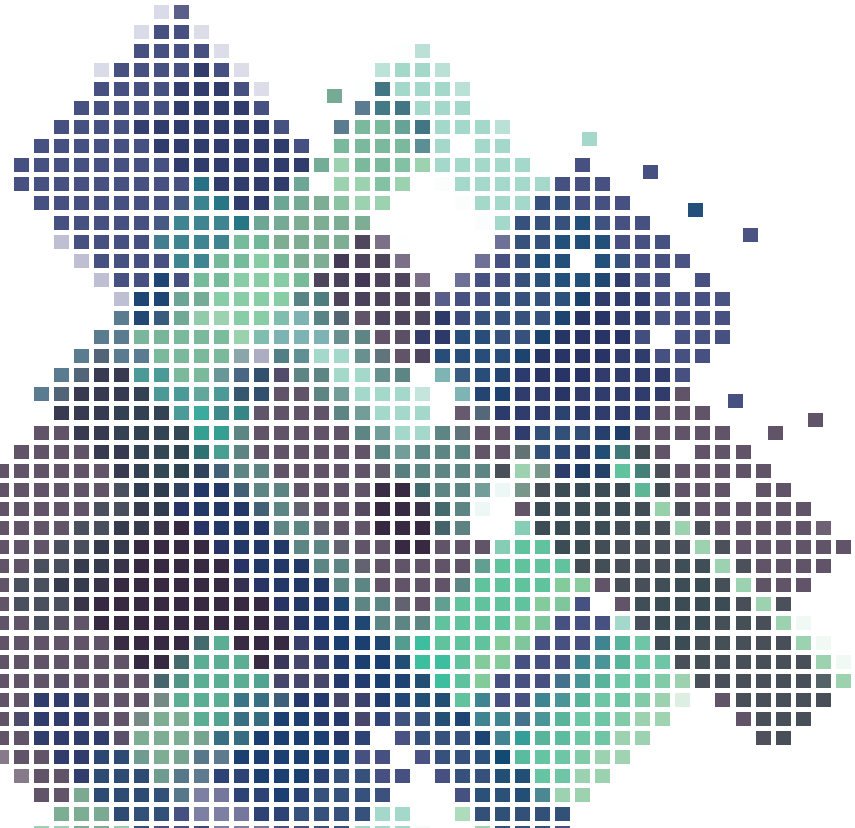
iKeepSafe
PEACE OF MIND FOR FAMILIES ONLINE™

Berkman
The Berkman Center for Internet & Society
at Harvard University

# Safety, Privacy, and Digital Citizenship

## *High School Curriculum*



DIGITAL LITERACY

TOOLKIT

# Safety, Privacy, and Digital Citizenship

Young people use technology in every aspect of their personal lives. To empower young people to be better digital citizens, we must seek to integrate digital literacies into their educational lives as well. In engaging this dialogue, across subject areas, we must take into account the importance not only of coding literacy, but also of web literacy and privacy management more broadly. In terms of managing privacy among peers, web-fluent young people can be extraordinarily savvy; however, like many adults, they may also incur risks that are not immediately apparent to them, in part from a lack of understanding of how large and enduring their digital footprint can be.

Through interactive activities and peer-facilitated discussion, students will be able to define key safety, privacy, and digital citizenship concepts and make more informed decisions about managing their personal information online. This curriculum is designed as a series of 15-20-minute lesson plans, which you can use as we have laid out, or in a fashion that best suits your own needs. All activities are modular, and the curriculum is licensed under a Creative Commons Attribution 3.0 Unported License, which means that you can share freely and remix the lessons—as long as you credit us. Please remix!


## Acknowledgements

BCIS thanks the Digital Literacy Toolkit team for their efforts on this curriculum: Sandra Cortesi, David Cruz, Urs Gasser, Paulina Haduong, Andres Lombana-Bermudez, Jeremiah Milbauer, Leah Plunkett, Dalia Topelson Ritvo, and Zoe Wood.

The Digital Literacy Toolkit team at BCIS would like to thank the following people and organizations for their valuable input and support.

- The Digital Media and Learning Research Hub Trust Challenge, supported by the MacArthur Foundation and administered by HASTAC.
- Our collaborators in the Digital Literacy Toolkit: MIT Scratch, New York Public Library, Press Pass TV, NuVu, the Engagement Game Lab, and the Walnut Hill School.
- Common Sense Media
- ConnectSafely
- Phillips Academy Andover
- Claudia L'Amoreaux

We would like to extend special thanks to our collaborator iKeepSafe for their input and feedback, particularly in sharing their Privacy Curriculum Matrix K-12 BEaPRO™ with us as guidance for developing this curriculum, which is available online at http://ikeepsafe.org/privacy-k-12-curriculum-matrix.


## National Standards

We have sought to align this curriculum to the greatest extent possible to the relevant standards from the Common Core English Learning Arts, American Association of School Librarians, and International Society of Technology Education. Because the creation of digital literacy and safety curricula is still a relatively new field, not all standards are precisely on point in terms of the content and skills we seek to cover. We encourage user feedback in this area in particular.

## Next Steps

We are releasing curricular modules in a series of small batches in order to best integrate and respond to collaborator and user feedback on content and design. (Please consult the Berkman Center's Digital Literacy Resource Platform, online at http://dlrp.berkman.harvard.edu, for module availability. All modules will be posted there as they are released.) This document—and those to follow shortly—represents our first version. We understand curricular design to be an inherently iterative process, so we'd love to know what kinds of improvements you're making, as well as what your students liked and didn't like. We expect to release updated versions going forward and would be delighted to incorporate your feedback. For questions or feedback, please contact Paulina Haduong at the Berkman Center at phaduong@cyber.law.harvard.edu.

# Core Topics
## Grades 9-10

### Concepts and Competencies
- Balance: Maintaining a healthy balance between online and offline activities
- Ethical Use: Making ethical decisions, being considerate of others and understanding potential consequences of online behavior
- Privacy: Protecting personal information and that of others
- Relationships: Engaging in safe and healthy online connections
- Reputation: Building a positive and truthful online presence that will contribute to future success
- Online Security: Using good habits for securing hardware and software

### Topics
- Awareness: Why does privacy matter?
- Protection: How can I protect myself?
- Data Collection and Boundaries: What are some of the legal and ethical boundaries of data collection?
- Sharing: How can I only share information with whom I want? How do I protect my reputation?

### Workshop Modules[1]
Note: These modules can be taught in any sequence, so feel free to mix and match!
- Intro to Privacy in the Digital Age [45 min]
- Passwords [30 min]
- Respect & Boundaries [15 min]
- Social Media and Sharing [30 min]
- Gaming and Online Privacy [35 min]
- Reputation [20 min]
- Mobile Location Security [20 min]
- Facial Recognition [25 min]
- Flirting & Sexting [15 min]
- Public Wifi [15 min]
- Data Collection & Terms of Service [35 min]
- Monitoring & Surveillance [30 min]
- Cyberbullying [20 min]
- Email [23 min]
- Anonymity & Online Identities [24 min]
- Cybersecurity, Phishing, & Spam [17 min]

### General extension activities
- Students could create videos or other creative projects to teach others about privacy.
- Students could also create lesson plans and teach younger grades about privacy issues.

---

1 The following modules, including accompanying handouts, are based on the framework found in the Volunteer Privacy Educators Program Curriculum developed by the Center for Law and Information Policy at Fordham University: Intro to Privacy in the Digital Age, Changing Contexts of Privacy, Passwords, Social Media and Sharing, Gaming and Online Privacy, Reputation, Flirting & Sexting, Mobile Location Security, Facial Recognition, and Public Wifi. Specific excerpts or quotations from the Volunteer Privacy Educators Program Curriculum ("CLIP Curriculum") appear in quotation marks and are cited in the modules and handouts where they appear. The CLIP Curriculum is available online in two parts (1) Lesson Plan Outlines, http://www.fordham.edu/downloads/file/4336/vpe_lesson_plan_outlines ("CLIP Curriculum Lesson") and (2) Teacher Training Manual, http://www.fordham.edu/downloads/file/4333/vpe_teacher_training_manual ("CLIP Curriculum Teacher").

# Tracks

Three big ideas explored in the curriculum are privacy, safety, and reputation. Below we've assembled a collection of modules to be taught to specifically focus on one topic. Each track includes a debate activity that explores an issue within each topic. Modules with bolded titles are considered crucial to these tracks, while other modules may reinforce and complement the material.

## Privacy

- **Intro to Privacy in the Digital Age**
- **Changing Contexts of Privacy**
- **Respect & Boundaries**
- **Social Media & Sharing**
- Gaming and Online Privacy
- Mobile Location Security
- Facial Recognition
- **Data Collection & Terms of Service**
- **Monitoring & Surveillance**
- Anonymity & Online Identities
- **Debate: Surveillance**

## Safety

- **Passwords**
- Gaming and Online Privacy
- **Flirting & Sexting**
- **Public Wifi**
- **Monitoring & Surveillance**
- **Cyberbullying**
- Anonymity & Online Identities
- **Cybersecurity, Phishing, & Spam**
- **Debate: Free Speech & Hate Speech**

## Reputation

- **Respect & Boundaries**
- **Social Media & Sharing**
- **Reputation**
- **Flirting & Sexting**
- **Anonymity & Online Identities**
- **Debate: Right to be Forgotten**

# Curricular Integration

There are exciting opportunities to teach this material every day in the classroom, even if you are not in a position to teach the entire curriculum. We have listed some ideas of potential teaching moments below and encourage educators to explore how they might integrate the issues and ideas presented in this curriculum into their existing lessons. Whenever you encourage or require students to go online when teaching this or other material, please keep in mind that you will want to make sure any online activity is consistent with any school, district, or other applicable policies, as well as any applicable privacy laws and regulations.

## General

- **Changing Context of Privacy:** Whenever you use an external application (such as a class blog, social networking platform, or technology explicitly designed for education), it presents an opportunity to discuss what you share online and the role of privacy norms. You can also work in some of the consequences of sharing online from other modules (including "Reputation" and "Social Media & Sharing").
- **Passwords:** Whenever you log into an external application in front of your students and/or ask your students to log in, you have a good opportunity to discuss how best to construct, share, and manage passwords. You use "Cybersecurity, Phishing, & Spam" to teach about the risks of being unsafe online.
- **Reputation:** When discussing future opportunities for students, whether jobs or college, it is important to emphasize how one's online reputation can play an important role.
- **Cyberbullying:** Online harassment is a serious threat to young people. Whenever discussing safety or bullying, this module can be useful.
- **Email:** If you are using email for your class and you are not sure if all your students are familiar with it, this module can make sure everyone is on the same page. This module can also be a useful opportunity for students to help their parents or extended relatives with email.

## STEM

- **Social Media & Sharing:** Whenever discussing networks and how things are spread through them (ideas, diseases, physical matter, etc.), social networks are useful prototypes. Topics discussed in this section can be used to help teach or reinforce the material.
- **Flirting & Sexting:** When teaching sexual education, this topic is useful to help educate young people about potential threats to their safety.
- **Public Wifi:** Wifi operates using physical signals, which could be elaborated on in a science class. Discussing waves or frequency is a good opportunity to discuss how wifi works.

## Social Studies

- **Monitoring & Surveillance:** When teaching American history, you can tie in the lessons from this module to teach about the Fourth Amendment.
- **Debate:** Free Speech & Hate Speech: When teaching American history, you can tie in the lessons from this module to teach about the First Amendment.

### Language

- **Social Media & Sharing:** Consider encouraging students to start a blog for short writing assignments. Students should consider how to share media online and its potential effects, both positive and negative.

### Art

- **Social Media & Sharing:** Consider encouraging students to share their work via social media (i.e., YouTube, Soundcloud, Deviant Art, etc.).Students should consider how to share media online and its potential effects, both positive and negative.

# Understanding Privacy
## Teacher Edition

This evaluation allows students to reflect on what they've learned through the course. Students should take this before and after the course and be able to review their answers. The extended explanations for the answers provided here should only be shared the second time. You may eliminate any questions that relate to material you do not plan to cover.

1. How do you define privacy online? | *Changing Contexts of Privacy*
2. Does privacy matter to you? Why? | *Changing Contexts of Privacy*

These questions should prompt students to reflect on their concepts of privacy, before and after the course. This idea should evolve as they consider new notions of privacy.

3. Which of the following is the strongest password? | *Passwords*
    a. password
    b. thisisaLOngpasswOrd!
    c. password12345
    d. 2016passWord

This password is the strongest because it mixes lowercase and uppercase letters, uses numbers (i.e., '0'), uses special characters (i.e., '!'), has many characters, and is easy to remember. None of these passwords are especially good, however, since 'password' or derivations of it are some of the most common passwords and can be easily guessed by a computer.

4. In which situation would it be okay to store your username/password on a computer so you can log in faster? | *Passwords*
    a. At the Apple Store
    b. At your local library
    c. In the computer lab where you sit every day
    d. At your best friend's house
    e. None of the above

Any computer that you do not use exclusively should not store any username or password information. If you have a dedicated account on a shared computer, this may be an acceptable option. However, if the account is shared, then that information is accessible by anyone who uses the computer. C is a good answer only if the shared computer has a personal account that you only have the password to. Otherwise, the best answer is E.

5. What is behavioral advertising? | *Changing Contexts of Privacy*
    a. When companies use ads to try to change your behavior.
    b. When companies collect data about who you are, what you are interested, and what you have been looking at online, then use that information to show you ads that they think will appeal to you.
    c. When companies allow you to create your own ad and put that on TV
    d. When companies put their ads everywhere: on billboards, TV, radio, Twitter, Facebook, Spotify, etc.

6. If you give your information to a company, they will never share that information with anyone else. | *Data Collection & Terms of Service*

a. True
b. False
c. Don't know/Don't care

Companies should tell you whether or not they share your information with others in their Terms of Services, which vary from company to company. To know how your information is being used, you must read a company's Terms of Service. You tell the company you have read and agree to the Terms of Service when you create an account with the website, even though most people just say they agree without reading the terms.

7. Which of the following might be able to get access to the location data on your smartphone? | *Mobile Location Security*

a. The company that makes the app you are using to check in (Yelp, Facebook, Foursquare, etc…)
b. The company that makes your phone (Apple, Motorola, HTC, Samsung, etc…)
c. Your phone company (Verizon, AT&T, T-Mobile, etc…)
d. All of the above
e. None of the above

8. Which of the following statements are true? | *Mobile Location Security*

a. Sharing your location data can be useful OR harmful.
b. You should never let your smartphone figure out your location because it's dangerous.
c. You don't need to worry about location data because it can ONLY be used to show you things you want to know.
d. All of my location data is available online anyway so I might as well share my location on social media.
e. By law, all apps must erase your location data after 10 days.

While students may personally feel that some of the other options are true for them, there are benefits and costs for sharing location data. Privacy is a personal decision, and each person will choose how to weigh those costs and benefits to decide what is right for herself or himself.

9. Who might see a comment you make on your friend Sarah's Facebook status? | *Social Media & Sharing*

a. Sarah
b. Sarah and Sarah's friends
c. Sarah, Sarah's friends, and your friends
d. Sarah, Sarah's friends, your friends, and the friends of Sarah's friends
e. Sarah and your friends

D covers all the people who could see the status. However, privacy controls can limit the group of people who can view material. It depends entirely on Sarah's privacy settings.

10. What is the best way to deal with Google search results about you that you don't like? | *Reputation*

a. Write an email to Google telling them to take it down.
b. Manage and create new content about yourself that will go above it.
c. Write an email to the administrator of the website you don't like.
d. All of the above.
e. There is nothing you can do about it.

Google is not likely to remove search results about you that you don't like, but the other two strategies can be effective. However, Google will help those who are victims of 'revenge porn' (sexually explicit content designed to intimidate, embarrass, or harass the person depicted).

11. What might you say to a friend who asks you to send them a sexual photograph? What if it's your romantic partner (ie. boyfriend, girlfriend, etc.)? Why? What are the risks? | *Flirting & Sexting*

These responses can be personal, but there are a few points to emphasize. It is typically illegal for minors to take and share nude photos, even of themselves. While sexting can be an intimate act for adult couples, companies host those photos and can sometimes fail to keep them secure. Additionally, the recipient of the photos may fail to keep them secure or may deliberately share the photos with others. If those photos are shared electronically, it is incredibly difficult to remove them.

12. You can be anonymous online, making it difficult for anyone monitoring your behavior to know who you are. | *Monitoring & Surveillance, Anonymity & Online Identities*

a. True
b. False
c. Don't know

It is possible to be entirely anonymous online, which has many implications. It is difficult to hold an anonymous user accountable for their actions and prevent them from repeatedly causing harm. However, there are legitimate reasons to be anonymous online. It should be noted that law enforcement can sometimes determine who anonymous users are, depending on what tools they are using to keep themselves anonymous.

13. Who could respond to inappropriate online activity? | *Cyberbullying*

a. Parents
b. Teachers
c. Peers
d. Police
e. All of the above
f. None of the above

Cyberbullying can be dealt with by intervention at many levels. If you or someone you know is the victim of cyberbullying, you should reach out to one or many of these groups.

14. Why would you use your real name online? | *Anonymity & Online Identities*

When developing a reputation for yourself online, using your real name is important. If someone searched for your name, you may want them to find certain content that you created. You can only do this by associating your real name with your online activity.

15. It is possible that websites will ask me for my password over email. | *Cybersecurity, Phishing, & Spam*

a. True

b. False

c. Don't know

It is standard procedure never to ask for a password over email. You should NEVER share a password over email. Emails may not be safe from a hacker or someone snooping through your email. Additionally, anyone asking for your password over email may be pretending to be the website. This person then may abuse your password once you've shared it with him or her.

# Understanding Privacy
## Evaluation

1. How do you define privacy online?

2. Does privacy matter to you? Why?

3. Which of the following is the strongest password?
    a. password
    b. thisisaL0ngpassw0rd!
    c. password12345
    d. 2016passWord

4. In which situation would it be okay to store your username/password on a computer so you can log in faster?
    a. At the Apple Store
    b. At your local library
    c. In the computer lab where you sit every day
    d. At your best friend's house
    e. None of the above

5. What is behavioral advertising?
    a. When companies use ads to try to change your behavior.
    b. When companies collect data about who you are, what you are interested, and what you have been looking at online, then use that information to show you ads that they think will appeal to you.
    c. When companies allow you to create your own ad and put that on TV
    d. When companies put their ads everywhere: on billboards, TV, radio, Twitter, Facebook, Spotify, etc.

6. If you give your information to a company, they will never share that information with anyone else.
    a. True
    b. False
    c. Don't know/Don't care

7. Which of the following might be able to get access to the location data on your smartphone?
    a. The company that makes the app you are using to check in (Yelp, Facebook, Foursquare, etc...)
    b. The company that makes your phone (Apple, Motorola, HTC, Samsung, etc...)
    c. Your phone company (Verizon, AT&T, T-Mobile, etc...)
    d. All of the above.
    e. None of the above

8. Which of the following statements are true?
   a. Sharing your location data can be useful OR harmful.
   b. You should never let your smartphone figure out your location because it's dangerous.
   c. You don't need to worry about location data because it can ONLY be used to show you things you want to know.
   d. My location data is available online anyway so I might as well share my location on social media.
   e. By law, all apps must erase your location data after 10 days.

9. Who might see a comment you make on your friend Sarah's Facebook status?
   a. Sarah
   b. Sarah and Sarah's friends
   c. Sarah, Sarah's friends, and your friends
   d. Sarah, Sarah's friends, your friends, and the friends of Sarah's friends
   e. Sarah and your friends

10. What is the best way to deal with Google search results about you that you don't like?
   a. Write an email to Google telling them to take it down.
   b. Manage and create new content about yourself that will go above it.
   c. Write an email to the administrator of the website you don't like.
   d. All of the above.
   e. There is nothing you can do about it.

11. What might you say to a friend who asks you to send them a sexual photograph? What if it's your romantic partner (ie. boyfriend, girlfriend, etc.)? Why? What are the risks?

12. You can be anonymous online, making it difficult for anyone monitoring your behavior to know who you are.
   a. True
   b. False
   c. Don't know

13. Who could respond to inappropriate online activity?
   a. Parents
   b. Teachers
   c. Peers
   d. Police
   e. All of the above
   f. None of the above

14. Why would you use your real name online?

15. It is possible that websites will ask me for my password over email.
   a. True
   b. False
   c. Don't know