Privacy Curriculum Matrix K-12 BEaPRO™

Core Privacy Concepts and Competencies:

Balance: Maintaining a healthy balance between online and offline activities.

Ethical Use: Making ethical decisions, being considerate of others and understanding 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.

Overview:

Privacy issues often don't have clear right and wrong answers. It is best to provide students with age-appropriate information and then allow them to think for themselves and reach their own conclusions about what best suits their values and comfort levels. Ideally, students should be taught through concrete examples, problems, and role-playing activities.

The curriculum must challenge students with material that is sophisticated and rich, not overly simplistic. The goal is to bring students to a better understanding of the consequences of exposing their own personal information and to help them understand the importance of respecting the privacy of others.

CORE ISSUES

I: AWARENESS
GENERAL PRIVACY AWARENESS

A. Issues

Privacy in the Digital Age

Students should learn that a lot of personal data is being collected about them and that it is being used in ways that may affect their lives and the lives of their families. Students should have an understanding of what privacy is. The challenge, then, is to make privacy a tangible idea, and not a vague and elusive concept.

Privacy consists of many interrelated ideas, behaviors and concerns. Most commonly, it involves protecting confidentiality. But it also involves not being snooped upon, not having one's identity exploited by others for their own aims, being informed about the data gathered about a person and how it will be used, having the ability to access data and correct errors, being able to prevent certain uses of data without consent, and much more.

Students should also think about the importance of privacy and how to reconcile it with competing interests. Why does privacy matter? How should difficult tradeoffs be made between privacy and free speech, effective law enforcement, efficient consumer transactions, and other values? The goal isn't to come up with all the answers, but to spark discussions and help students understand the issues more deeply and more completely.

Students should also learn about the potential dangers and consequences that can follow from disclosing personal data, as well as the harms they can cause when they invade the privacy of others.

Use of Online Services and Products

Students use many websites and online services without understanding the privacy implications. Students should learn how readily information can be gathered simply as a result of using technology and the importance of learning how that information might be used, so that they can consider how to balance both the benefits and risks of online technologies

Students should be taught to locate, read and understand the terms of use and privacy policies of online services before they sign up. Students should consider what boundaries they might want to set around information sharing on each site or service that they use. They should also learn how to customize their privacy settings on any platform and how to exercise their choice to opt out of disclosing information, if they want to.

Students often have a poor understanding of the true costs of "free" online services. Students should learn that many "free" online services are not completely free, but are instead offered to users at no cost in exchange for the use of their personal data. To this end, students should learn how online services go about monetizing their personal data.

Students should also learn to appreciate the need to pause and think before disclosing information online. They should be helped to understand how easy it can be to disclose information or post something that they might regret later on. For example, consider the many misguided statements made by celebrities online that they later retract and apologize for, or how what may have been intended to be a harmless comment made online can sometimes result in a friend's feelings being hurt.

B. Objectives

AWARENESS	K-3	4-8	9-12
Data collection: What can be learned by gathering lots of data?	I can cite examples of how people make correct and incorrect inferences about what they see online. I describe how pictures and messages may have more information in them than I realize.	I can describe how people make right and wrong inferences online. I describe how pictures and messages may have more information in them than I realize.	I can evaluate the consequences of information sharing and making inferences. I describe how pictures and messages may have more information in them than I realize.
Nothing to hide: Why does privacy matter?	I decide with my family what I want to keep private. In addition, I keep private: My full name My address My phone number My school (name/address) Other places I go regularly Where I am	I decide what I want to keep private. I recognize that people have different ideas about what they want to keep private. I respect the privacy decisions of others.	I decide what I want to keep private. I recognize that people have different ideas about what they want to keep private. I respect the privacy decisions of others.
Online terms of use and privacy policies	I only sign up for things online with an adult's help. I can locate the terms of use and privacy policy before using online services.	I can customize my privacy settings for the online services I use. I assess how my data is being used by each online service. I make decisions about information sharing with each site I use. I can identify when I am trading my personal information for free services. I understand the reason for the terms of use and privacy policy	I can customize my privacy settings for the online services I use. I assess how my data is being used by each online service. I make decisions about information sharing with each site I use. I can identify when I am trading my personal information for free services. I can describe how websites generate revenue. I can read and understand the terms of use and privacy policy before using online services.

Vocabulary	Privacy Data Inference Terms of Use	Privacy Data Inference Snoop Information Boundary Terms of Use Privacy Policy Report Abuse Privacy Settings	Privacy Data Inference Snoop Information Boundary Terms of Use Privacy Policy Privacy Settings Report Abuse Disclose/disclosure Revenue/Monetize

C. Activities

1. Data Collection: What can be learned by gathering lots of pieces of data?

AWARENESS	K-3	4-8	9-12
Data collection: What can be learned by gathering lots of data	I can cite examples of how people make correct and incorrect inferences about what they see online. I describe how pictures and messages may have more information in them than I realize.	I can describe how people make right and wrong inferences online. I describe how pictures and messages may have more information in them than I realize.	I can evaluate the consequences of information sharing and making inferences. I describe how pictures and messages may have more information in them than I realize.

Have students identify all the ways information can be collected about people. Create a fictitious character and have students tell us what information they find out about him/her. Create various materials where this information can be located – a social media profile, a list of credit card purchases, a credit report, a list of URLs visited, etc. Younger children might be provided with a box of items and toys that another person owns.

Discussion: What kind of inferences can be made from looking at this data together? What can we learn about the character by looking at the data?

Then show the truth about the character. Some of the inferences will be correct, but some might be incorrect. This will show that inferences are not always accurate but might still be used to judge a person or make decisions about a person.

Basic Lesson: A lot can be learned by piecing together information about a person. But not all inferences made based on this data may be correct.

The next step in this exercise is to consider the consequences.

Discussion: Does the character want someone to know all this data? How might the data be used? Have students discuss how various people or organizations might use the data, such as: (1) parents; (2) college admissions officers; (3) employers; (4) friends; (5) the police; (6) an insurance company; (7) a bank loan officer and (8) data miners / marketers

Advanced Lesson: The goal of this activity is to help students learn that all the pieces of data they expose can reveal more than they might intend, and they should be mindful of this fact and the potential consequences.

2. Nothing to Hide: Why does privacy matter?

AWARENESS	K-3	4-8	9-12
Nothing to hide: Why does privacy matter?	I decide with my family what I want to keep private. In addition, I keep private: My full name My address My phone number My school (name/address) Other places I go regularly Where I am	I decide what I want to keep private. I recognize that people have different ideas about what they want to keep private. I respect the privacy decisions of others.	I decide what I want to keep private. I recognize that people have different ideas about what they want to keep private. I respect the privacy decisions of others.

Use a video or story to show that privacy is about more than hiding secrets. Potential ideas for scenarios:

- Character gets bitten by a weird insect that causes an ugly multi-colored rash on his/her stomach. Doesn't want others to know. Discuss: Should others know?

- Character writes a diary. Another person scans it in and posts it online. Discuss: Does the character have a right to privacy in his/her diary? Was the other person wrong to post it online?

- A person secretly watches character via remote access to his/her webcam. Discuss: Is this appropriate? Creepy? What are the consequences of such snooping? Could be a criminal violation and lead to jail time.

- Character receives a bonus at work. Another character makes a post about being taken out to dinner to celebrate the character's bonus. This example (1) recognizes that sharing even good information about someone else can be an invasion of privacy; and (2) recognizes the way we inadvertently reveal information about others without intentionally meaning to harm/embarrass them.

- Character posts "have a good vacation" on a friend's social media page. Discuss: What if the friend didn't want anyone to know he/she was going away? Are there alternative more private ways to communicate this message (i.e. sending a private message or text)?

- Character is a cancer survivor. A friend reveals this fact about the character online. Discuss: Imagine one person who wants to reveal this information to others. Why might the character want it to be known? Imagine another person who doesn't others to know. Why might the character not want it to be known?

Discussion: Is it wrong to hide secrets? Why do people keep secrets? Is it wrong to snoop into people's lives and learn secrets they don't want known? Is it wrong to disclose people's secrets to others? What are some examples of things that people might want to keep secret? What are some examples of things that should not be kept secret?

Lesson: The goal of this activity is to teach students that it is important to consider that everyone may not have the same desires for privacy and we should respect each other's privacy.

3. Online Terms of Use and Privacy Policies

AWARENESS	K-3	4-8	9-12
Online terms of use and privacy policies	I only sign up for things online with an adult's help. I can locate the terms of use and privacy policy before using online services.	I can customize my privacy settings for the online services I use. I assess how my data is being used by each online service. I make decisions about information sharing with each site I use. I can identify when I am trading my personal information for free services. I understand the reason for the terms of use and privacy policy	I can customize my privacy settings for the online services I use. I assess how my data is being used by each online service. I make decisions about information sharing with each site I use. I can identify when I am trading my personal information for free services. I can describe how websites generate revenue. I can read and understand the terms of use and privacy policy before using online services.

Examine a real privacy policy or terms of use of a popular online service to see how much a person gives up when they use that service. Have students identify which terms are problematic and why.

This activity is more appropriate for middle school and up. But earlier grades can still be taught the underlying lesson by being asked whether they will do something or accept something if the terms aren't good. Example: Kids are given 3 stickers. They can get a 4th sticker if they agree to a set of terms. One term is that they must give up 2 stickers.

Lesson: The goal of this activity is to teach students that there are terms and policies attached to website and online services that control the ways in which we can use the services and what expectation of privacy we have when doing so. Students should learn from early on that they should always check to see what they might be giving up when using a service. They should learn to look at the fine print. This is a lesson so few know as adults, so it is important that it be instilled early on.

II: PROTECTION
SAFETY AND SECURITY

A. Issues

Identity Theft

Identity theft is becoming more prevalent and can cause great damage. Identity theft is a growing problem for children because parents do not often check credit reports for their children, and the theft is likely to go undetected for a longer period of time. Students should learn what identity theft is, steps that can be taken to help prevent it, and how to deal with identity theft if they are victimized.

Phishing and Online Threats

Students should learn how to recognize phishing attempts and how to avoid providing personal data to fraudsters. Students should learn about online threats such as viruses, spyware, and other malware and how to avoid being victimized. Students should also learn about spear phishing – the technique of using personal data about a person found online to make that person think that the phisher knows them.

Privacy and Physical Safety

Just as students are taught to be careful when interacting with strangers offline, they should also be taught the same lessons about interacting with strangers online. Students should learn how, in rare instances, disclosing personal data may compromise their physical safety, such as creating risks of kidnapping, molestation, and other harms. Disclosing one's address and location (either purposely or inadvertently, such as posting photos with geolocation) can be dangerous. Students should understand the studies indicating that youth who send personal information (such as photos, names or telephone numbers) to strangers online are more likely to receive requests for actual or offline contact. Students should understand how accepting friend requests from "friends of friends" can be the same as accepting one from a stranger.

Black-and-white approaches, such as "never give out personal data online" or "never interact with strangers online," are ineffective because they are too broad and fail to recognize that most youth will inevitably give out personal information or interact with strangers without negative repercussions.
Instead of blanket "never" statements, students should be taught to be careful about sharing location information (intentionally or unintentionally) and to be aware that discussing sex online, especially with strangers can be a red flag for danger.

Data Security

Students should learn about good data security practices so that their personal data doesn't fall into the wrong hands and that they don't expose their data or computers to undue risk. Beyond being aware of phishing attempts, students should learn about social engineering, the risks of putting sensitive data on portable devices, the importance of backing up important data, how to encrypt data, how to select good passwords and change them regularly, the importance of not sharing passwords, how to properly dispose of data, how to password-protect devices such as phones and tablets, and how to surf the Web safely.

B. Objectives

PROTECTION	K-3	4-8	9-12
Selecting Good Passwords	I only share my passwords with my parents/guardians and teacher. I password protect my devices. I change my passwords regularly. I create passwords with an adult that are hard to guess and easy to remember using songs, numbers, and symbols. I can use: 3 for E # for H 5 for S + for T	I only share my passwords with my parents/guardians. I password protect my devices. I change my passwords regularly. I create passwords that are hard to guess and easy to remember using phrases, numbers, symbols, and upper- and lowercase letters. I use multi-factor authentication when possible.	I only share my passwords with my parents/guardians. I password protect my devices. I change my passwords regularly. I create passwords that are hard to guess and easy to remember using phrases, numbers, symbols, and upper- and lowercase letters. I use multi-factor authentication when possible.
Avoiding Phishing Tricks	I recognize the signs of phishing attempts. I tell an adult if I receive a strange email or phone call. Before sharing any personal information online or over the phone (like my address), I ask a parent or guardian for help.	I can list different techniques people use to steal identities. I can describe how to prevent identity theft. I know whom to call if I think I'm a victim of identity theft. I recognize the signs of phishing attempts. I am careful about how, when, and with whom I share personal information.	I can list and describe different techniques people use to steal identities. I can describe how to prevent identity theft. I know whom to call if I think I'm a victim of identity theft. I recognize the signs of phishing attempts. I am careful about how, when, and with whom I share personal information.
Identify Security Risks	I ensure that I only interact with trusted websites with help from an adult.	I recognize online security risks and how to respond appropriately.	I recognize online security risks and how to respond appropriately.

(continued on next page…)

Online Impersonation	I am honest online. I recognize that strangers come in many forms. I understand my parent or guardian's rules about who I may connect with online. I let an adult know if someone tries to discuss something online that makes me uncomfortable.	I am honest online. I recognize that my audience online may be bigger than I expect. I take steps to confirm that I really know the identity of the people I talk/chat/text/connect with online. I ask follow-up questions and/or seek help from an adult if I'm unsure. I stop and think before I friend or connect online with someone. I am careful about whom I give personal information to and what kinds of things I share. I tell an adult if someone tries to discuss something online that makes me uncomfortable.	I am honest online I am careful when sharing my devices with friends I recognize that my audience online may be bigger than I expect. I take steps to confirm that I really know the identity of the people I talk/chat/text/connect with online. I ask follow-up questions and/or seek help from an adult if I'm unsure. I stop and think before I friend or connect online with someone. I am careful about whom I give personal information to and what kinds of things I share. I tell an adult if someone tries to discuss something online that makes me uncomfortable
Vocabulary	Phishing Hacker Impersonation Password	Identity Theft Phishing Viruses Spyware Malware Hacker Data Security Impersonation Password Encryption Multi-factor authentication	Identity Theft Phishing Viruses Spyware Malware Hacker Data Security Impersonation Password Encryption Multi-factor authentication

C. Activities

1. Outsmart the Hacker: Selecting Good Passwords

PROTECTION	K-3	4-8	9-12
Selecting Good Passwords	I only share my passwords with my parents/guardians and teacher. I password protect my devices. I change my passwords regularly. I create passwords with an adult that are hard to guess and easy to remember using songs, numbers, and symbols. I can use: 3 for E # for H 5 for S + for T	I only share my passwords with my parents/guardians. I password protect my devices. I change my passwords regularly. I create passwords that are hard to guess and easy to remember using phrases, numbers, symbols, and upper- and lowercase letters. I use multi-factor authentication when possible.	I only share my passwords with my parents/guardians. I password protect my devices. I change my passwords regularly. I create passwords that are hard to guess and easy to remember using phrases, numbers, symbols, and upper- and lowercase letters. I use multi-factor authentication when possible.

After being taught about how to select good passwords, students play a game where they try to select the best password.

Lesson: The goal of this activity is to teach students how to choose good passwords.

Students should also be taught not to share passwords with anyone but their parents (or other trusted adult), and not to keep their passwords forever, but to change them regularly.

Another activity might include having students construct good passwords that they can remember. They might take some words and change the case of letters and add numbers and special characters. They must also create one that they can remember because if they write the password down in a note in their wallet, then the good password is for naught. For example, a student chooses two or three short words: Dog, Cat, Rat. Then add numbers: Dog2Cat8Rat. Then add special characters: Dog2Cat8Rat@. Another example: Come up with a phrase (with numbers) that you like such as "my Mom is 78 this year" and use the first letters to make your password: mMi78ty

One additional element that might be useful to add this activity: It could be developed into a competition where students not only have to come up with a good password that meets certain parameters but also with one that the student can remember. It is easy in an exercise to come up with a very complex password, but it is much harder to come up with a complex password that can readily be remembered.

2. Outsmart the Hacker: Avoiding Phishing Tricks

PROTECTION	K-3	4-8	9-12
Avoiding Phishing Tricks	I recognize the signs of phishing attempts. I tell an adult if I receive a strange email or phone call. Before sharing any personal information online or over the phone (like my address), I ask a parent or guardian for help.	I can list different techniques people use to steal identities. I can describe how to prevent identity theft. I know whom to call if I think I'm a victim of identity theft. I recognize the signs of phishing attempts. I am careful about how, when, and with whom I share personal information.	I can list and describe different techniques people use to steal identities. I can describe how to prevent identity theft. I know whom to call if I think I'm a victim of identity theft. I recognize the signs of phishing attempts. I am careful about how, when, and with whom I share personal information.

After being taught about how phishers try to trick people with fake emails, social media posts and phone calls, students play a game where they try to find the clues on various emails or phone calls that indicate they are phishing scams.

Spear phishing – phishing using a few pieces of personal data – is much more effective than generic phishing. Phishing exercises might employ using a few pieces of personal data that are readily obtainable online and seeing if students are more likely to be fooled. Students need to learn that in today's age, the use of personal data doesn't mean that an email is more trustworthy.

Lesson: The goal of this activity is to make students be very careful to look for anything odd or unusual in an email or phone call so they can avoid clicking or going to a dangerous website.

3. Identify Security Risks

PROTECTION	K-3	4-8	9-12
Identify Security Risks	I ensure that I only interact with trusted websites with help from an adult.	I recognize online security risks and how to respond appropriately.	I recognize online security risks and how to respond appropriately.

Game where students identify the security risks in a scene – kind of like finding Waldo.

Lesson: The goal of this activity is to teach students all the ways that data can be accessed and stolen.

4. Online Impersonation

PROTECTION	K-3	4-8	9-12
Online Impersonation	I am honest online. I recognize that strangers come in many forms. I understand my parent or guardian's rules about who I may connect with online. I let an adult know if someone tries to discuss something online that makes me uncomfortable.	I am honest online. I recognize that my audience online may be bigger than I expect. I take steps to confirm that I really know the identity of the people I talk/chat/text/connect with online. I ask follow-up questions and/or seek help from an adult if I'm unsure. I stop and think before I friend or connect online with someone. I am careful about whom I give personal information to and what kinds of things I share. I tell an adult if someone tries to discuss something online that makes me uncomfortable.	I am honest online I am careful when sharing my devices with friends I recognize that my audience online may be bigger than I expect. I take steps to confirm that I really know the identity of the people I talk/chat/text/connect with online. I ask follow-up questions and/or seek help from an adult if I'm unsure. I stop and think before I friend or connect online with someone. I am careful about whom I give personal information to and what kinds of things I share. I tell an adult if someone tries to discuss something online that makes me uncomfortable

Video or story illustrating how easy it is for someone to impersonate another online. In addition to focusing on the importance of not trusting a stranger online, students can be taught the ethics of impersonating others online and that doing so is wrong and can be against the law in some circumstances.

In early grades, this activity can focus on animal characters or Halloween costumes so it is not too distressing. Little Red Riding Hood is a good example of this – the Big Bad Wolf impersonates her grandmother, but there are clues. In later grades, a greater dose of realism should be included, to ensure students understand the potential dangers. Activities about impersonating others can be a little more relaxed, as online impersonation is sometimes done to taunt or mock, not to harm or molest.
Nevertheless, online impersonation is a serious issue, and in some cases can be illegal.

This lesson can also be applied to phishing attempts, where fraudsters impersonate emails from real companies or impersonate websites from real companies. So much online can be faked with ease. Most recently, after the Target data breach, fraudsters sent fake emails to people that looked like they came from Target notifying them about the breach and tricking them into providing personal data.

Another element of this activity might illustrate how information found online might not be trustworthy or accurate. Although people may know this in the abstract, they still in practice often trust more than they should. We might look to social science and behavioral economic literature to better understand the factors that make people trust and how to create a healthy skepticism.

This exercise must be balanced so that students do not become overly skeptical. Essentially, students need to learn about the kinds of data that only trusted real people will know and the kinds of facts that a fraudster or harm-doer might be able to find out and use. Students should be taught to ask follow up questions when in doubt to make sure that the person is bona fide.

III: COLLECTION

RESPECTING PRIVACY BOUNDARIES: SNOOPING AND OTHER FORMS OF DATA COLLECTION

A. Issues

Ethical Respect for the Privacy Boundaries of Others

Students should be taught to respect other people's boundaries for sharing their personal information, especially when these boundaries are different from one's own boundaries. Certain technologies make it easy to invade other people's privacy by taking a photo of people without their consent, secretly recording people, or snooping into personal online accounts or devices. It is important for students to understand that these technologies can make it easy to invade someone's privacy and that these technologies should be used with care.

People also might share photos and other personal information about others without asking their permission first. Students should understand the ethical implications of doing so, and appreciate that others might not want the exposure. Students should be taught the norm of asking for permission or finding out what other people want before disclosing photos or other information..

Legal Boundaries on Information Collection and Use

Students should be aware that certain privacy violations are illegal, and the penalties for a number of them include potential jail time. Video voyeurism and Peeping Tom activities are illegal in many states. Searching electronic devices of others without their consent is a federal crime (and often a state crime). Accessing private email or accounts of others is also a federal and state crime. Certain surveillance activities are also illegal, such as certain forms of audio and video surveillance – even when done in public. Students often think that anything their devices can do is legal, but there are many things that these powerful devices can do that can constitute very serious crimes.

Government Searches and Surveillance

Students should be taught about their basic rights as citizens when it comes to government searches and surveillance. People have constitutional rights under the Fourth Amendment that limit when and how the government can gather their personal data. The Fourth Amendment works generally by requiring that law enforcement officials go to a judge and obtain a warrant before they can engage in certain kinds of searches.

A warrant requires law enforcement officials to justify the search by showing probably cause (a reasonable basis to believe that they will find evidence of a crime in the places or things they want to search).

B. Objectives

COLLECTION	K-3	4-8	9-12
What harms are caused by snooping?	I ask permission before I go through someone's backpack/desk/computer/phone.	I can describe & avoid the many ways one might invade someone else's privacy.	I can describe & avoid the many ways one might invade someone else's privacy.
Ethics vs. law	I understand that just because I can do something, does not mean I should.	I understand that just because it's legal doesn't mean it's right.	I understand that just because it's legal doesn't mean it's right.
The 4th Amendment	N/A	I can explain how the 4th amendment relates to my technology use.	I can explain how the 4th amendment relates to my technology use.
Photo/Information boundaries	I respect other people's personal boundaries. I think about other's feelings before I capture or share something about them. I only record others with their permission. I can describe how sharing changes across different relationships: Doctor Teacher Parent Friend Stranger	I respect other people's personal boundaries. I think about other's feelings before I capture or share something about them. I only record others with their permission. I can describe how sharing changes across different relationships (eg. with family, with friend, with acquaintance, stranger, doctor)	I respect other people's personal boundaries. I think about other's feelings before I capture or share something about them. I only record others with their permission. I can describe how sharing changes across different relationships (eg. with family, with friend, with acquaintance, stranger, doctor)
Vocabulary	Boundaries Snooping	Boundaries Amendment Disclosure Search Surveillance Snooping	Boundaries Amendment Disclosure Search Surveillance Snooping

C. Activities

1. The Snooper: What harms are caused by snooping?

COLLECTION	K-3	4-8	9-12
What harms are caused by snooping?	I ask permission before I go through someone's backpack/desk/computer/phone.	I can describe & avoid the many ways one might invade someone else's privacy.	I can describe & avoid the many ways one might invade someone else's privacy.

Show video vignette where one person snoops into another's private life.

Discuss: How would that make the person feel? Why would the person not want the information known? What is wrong with snooping? What do you think about the snooper? Is the snooper acting ethically? Why is the snooper snooping? How would you feel if someone did it to you?

This might best begin after preschool, as I don't think preschoolers are particularly upset by snooping. When a sense of private space and private matters starts dawning on children, that is when this activity can work best. In late middle school and high school, students should also be taught about the legal implications – some forms of snooping are crimes.

Lesson: The goal of this activity is to make students think about why people want privacy, why snooping can create discomfort, and why snooping can make others angry and give the snooper a bad reputation.

2. Ethics vs. Law

COLLECTION	K-3	4-8	9-12
Ethics vs. law	I understand that just because I can do something, does not mean I should.	I understand that just because it's legal doesn't mean it's right.	I understand that just because it's legal doesn't mean it's right.

This might be too advanced, but a class might discuss whether certain legal restrictions on collecting or disclosing data match up to students' sense of the ethics of doing so. The law often doesn't match up precisely to ethics, and the conversation about what is ethical or not ethical and what should be prohibited by law is an interesting one. The law would need to be simplified for students, but there are ways that this exercise might be able to work.

3. Government Searches and Surveillance: The Fourth Amendment

COLLECTION	K-3	4-8	9-12
The 4th Amendment	N/A	I can explain how the 4th amendment relates to my technology use.	I can explain how the 4th amendment relates to my technology use.

Students might be taught a basic lesson about the Fourth Amendment. Although the Fourth Amendment is quite complex, there have been effective efforts to explain the basics to non-lawyers.

A fun exercise might be to focus on what the U.S. Supreme Court has decided constitutes a "reasonable expectation of privacy," which must exist in order for there to be Fourth Amendment protection. The Supreme Court's decisions on when there is a reasonable expectation of privacy are quite controversial and somewhat inconsistent. Students might be given a list of the various situations involved in the cases and asked whether they think there is a reasonable expectation of privacy. In an empirical study, the responses of people to these situations differed significantly from what the Supreme Court had held. This discussion does not require expertise in the law, and students can readily engage in interesting debates about whether the Supreme Court decided correctly or incorrectly.

This exercise is best suited for grades 8 and up.

4. The Photo

COLLECTION	K-3	4-8	9-12
Photo/Information boundaries	I respect other people's personal boundaries. I think about other's feelings before I capture or share something about them. I only record others with their permission. I can describe how sharing changes across different relationships: Doctor Teacher Parent Friend Stranger	I respect other people's personal boundaries. I think about other's feelings before I capture or share something about them. I only record others with their permission. I can describe how sharing changes across different relationships (eg. with family, with friend, with acquaintance, stranger, doctor)	I respect other people's personal boundaries. I think about other's feelings before I capture or share something about them. I only record others with their permission. I can describe how sharing changes across different relationships (eg. with family, with friend, with acquaintance, stranger, doctor)

Show video vignette where X takes Y's photo when Y is in an embarrassing position. Y might be crying. Or Y might have fallen into the mud and be embarrassed. Discuss: Why might Y not want his/her photo taken or

disclosed? In another scenario, perhaps Y simply wasn't comfortable with his expression in a particular photo. Discuss what might happen if X shared the photo with others without Y's permission.
The goal of this activity is to make students think about other people's feelings before they capture and/or share data about other people.

5. Information Boundaries

COLLECTION	K-3	4-8	9-12
Photo/Information boundaries	I respect other people's personal boundaries. I think about other's feelings before I capture or share something about them. I only record others with their permission. I can describe how sharing changes across different relationships: Doctor Teacher Parent Friend Stranger	I respect other people's personal boundaries. I think about other's feelings before I capture or share something about them. I only record others with their permission. I can describe how sharing changes across different relationships (eg. with family, with friend, with acquaintance, stranger, doctor)	I respect other people's personal boundaries. I think about other's feelings before I capture or share something about them. I only record others with their permission. I can describe how sharing changes across different relationships (eg. with family, with friend, with acquaintance, stranger, doctor)

Create a scenario where there are various facts about a character. Then there are the "knowers" -- classmates, friends, parents, siblings, teachers, doctor. What facts should be known by each type of knower? Students determine what facts each knower should know.

A video vignette about boundaries being broken down might also be effective. This type of situation is used to great effect in many TV situation comedies, where too much information is exposed to some people, and sometimes not enough information exposed to others. Or a person overhears partial information and misconstrues what is going on. These result in awkward messy situations.

The goal of this activity is to demonstrate that in different kinds of relationships, people want to expose different pieces of information, and this is reasonable and normal.

IV: SHARING

SHARING PERSONAL DATA ABOUT ONESELF AND OTHERS

A. Issues

Confidentiality

Students should be taught about the ethics of maintaining confidentiality of private information. Students should be taught that certain types of individuals owe more than just an ethical duty of confidentiality – they also owe a legal duty. These individuals include lawyers, doctors, accountants, government officials, and others. Additionally, students should be taught about when it is appropriate to breach confidentiality, especially when the health or safety of the person or others is at stake.

Examples include when a student knows that another has made a threat or that another has indicated they are contemplating suicide. Students should be taught how and with whom to share information under these circumstances.

Online Gossip and Self-Exposure

Students should be taught why gossip about others, especially online, can cause others significant harm. The golden rule about treating others the way you wish to be treated should be reiterated.

Students should learn that one of the best defenses to protecting their online reputation is to be careful about what they post online. Sharing information and photos with others is natural, but students must recognize that such sharing is accompanied by a loss of control over who else may see that information or photo.

Students should learn that there may be negative consequences to self-exposure (such as embarrassing photos or inappropriate language) including lost of job opportunities, scholarships or college admission. However, any lesson about the negative consequences must be accompanied by information that there are measures students can take if she/he later regrets making a post or if that post is shared beyond his/her intended audience. Students should learn that they can request website operators and hosts of the material to take down harmful or embarrassing information or photos of themselves and many will voluntarily do so. Many website have terms of use that prohibit posting certain information, so the offensive information is often a violation of these terms of use. In addition, depending upon how the information was created, students may have various legal tools to help them. For example, if a photo was posted about a student and the student was the one who took the photo, the student can use copyright law to take it down.

A careful balance must be struck between informing students that what is posted online can be forever and have consequences that last a lifetime. Students definitely need to understand the gravity of posting data online. On the other hand, a lot of information online does actually disappear and can be removed. This latter point is helpful because sometimes students who are cyberbullied or who have nude or embarrassing photos

or data posted online might feel that their lives are ruined forever and that might incline them to feel hopeless and contemplate suicide. The fact is that things are far from hopeless. The harm need not be permanent.

Cyberbullying and Online Harassment

Students should be taught the ways cyberbullying is different from traditional bullying. For example, the perpetrator/victim role may not be static; the audience is larger with a greater potential for embarrassment; and the harassment can occur at any time of the day or night. In addition, students should understand that, in some cases, online harassment has led to civil lawsuits and criminal penalties against the perpetrator. Moreover, the perpetrators can live a lifetime of regret. A significant amount of time should be spent teaching students how to help others who are targets of harassment and what they can do when they observe or experience online cruelty. They need to know how to respond and where to find resources and people who can help them.

Sexting and "Youth Produced Sexual Images"

Students should be taught about the potential dangers of sexting – writing sexually explicit messages or sending nude or sexually-explicit photos. Students who send, post, forward or take sexual explicit images of a minor are engaging in a potentially dangerous behavior that has the potential to cause reputational harm and emotional distress. In rare cases, sexting has led to child porn charges and sex offender registration for the offender and blackmail of the victim. Capturing and distributing nude images of adults can also carry civil and criminal legal penalties.

B. Objectives

SHARING	K-3	4-8	9-12
Confidentiality	I know the difference between tattling and responsible reporting. I tell an adult when someone is going to hurt himself or others or might get hurt. When a secret makes me uncomfortable, I tell an adult.	I know when to keep and when to break confidentiality. I know who to tell when I learn that someone is in harm's way or is going to cause others or himself harm.	I know when to keep and when to break confidentiality. I know who to tell when I learn that someone is in harm's way or is going to cause others or himself harm.

(continued on next page…)

Online disclosures	I treat others with respect online and in person. I explain why cyber- bullying is always wrong. I can identify the 3 different roles of a bullying encounter. I know what to do if I am the target or a bystander. I discuss how what I say about others is a reflection on me. I am honest.	I treat others with respect online and in person. I explain why cyber- bullying is always wrong and often illegal. I can identify the 3 different roles of a bullying encounter. I know what to do if I am the target or a bystander. I discuss how what I say about others is a reflection on me. I am honest. I understand the consequences of taking, sending, posting, or forwarding sexual images of a minor. (emotional, reputational, legal).	I treat others with respect online and in person. I explain why cyber- bullying is always wrong and often illegal. I can identify the 3 different roles of a bullying encounter. I know what to do if I am the target or a bystander. I discuss how what I say about others is a reflection on me. I am honest. I understand the consequences of taking, sending, posting, or forwarding sexual images of a minor or of an adult. (emotional, reputational, legal).
Self exposure online	I cultivate a positive online reputation. I recognize that when I share online, I do not control who can see what I share.	I cultivate a positive online reputation. I recognize that when I share online, I do not control who can see what I share. I know that an internet or mobile message can last a long time, even ones that claim to be temporary or self- destructing. I know how to get help if I need something removed. I can locate the "report" buttons and I use them when I see something harmful or inappropriate online. I explain what types of disclosures are appropriate and desirable and what types might not be. Before sharing something online, I should PAUSE **P** - Do I have **Permission** to post this? (Is it mine to share?) **A** - Is it **Accurate**? (Is it true/honest?) **U** - Is it **Useful**? (Why am I posting this? Will it help others, teach others, **S** - Is it **Safe** to share? (Is it too personal/private/sexual? Is it legal?) **E** - Whose **Eyes** Will See it? (Am I ok with who will see this? Do I know who I am sharing this with)	I cultivate a positive online reputation. I recognize that when I share online, I do not control who can see what I share. I know that an internet post can last a long time, even ones that claim to be temporary or self-destructing. I know how to get help if I need something removed. I can locate the "report" buttons and I use them when I see something harmful or inappropriate online. I explain what types of disclosures are appropriate and desirable and what types might not be. Before sharing something online, I should PAUSE **P** - Do I have **Permission** to post this? (Is it mine to share?) **A** - Is it **Accurate**? (Is it true/honest?) **U** - Is it **Useful**? (Why am I posting this? Will it help others, teach others, **S** - Is it **Safe** to share? (Is it too personal/private/sexual? Is it legal?) **E** - Whose **Eyes** Will See it? (Am I ok with who will see this? Do I know who I am sharing this with)

(continued on next page…)

Vocabulary	Confidentiality Cyber-bullying Cultivate	Confidentiality Exposure Gossip Cyber-bullying Harassment Cultivate Sexting Minor	Confidentiality Exposure Gossip Cyber-bullying Harassment Cultivate Sexting Minor

1. Confidentiality

SHARING	K-3	4-8	9-12
Confidentiality	I know the difference between tattling and responsible reporting. I tell an adult when someone is going to hurt himself or others or might get hurt. When a secret makes me uncomfortable, I tell an adult.	I know when to keep and when to break confidentiality. I know who to tell when I learn that someone is in harm's way or is going to cause others or himself harm.	I know when to keep and when to break confidentiality. I know who to tell when I learn that someone is in harm's way or is going to cause others or himself harm.

Video scenarios involving confidentiality. One might depict an unjustified breach of confidentiality. Discuss: What do you think of the friend who betrayed the secret? Can the friend be trusted? Did the friend act appropriately? Why would the person betrayed be upset or harmed?

Another video vignette might depict situations where a friend contemplates breaching confidentiality. Discuss: Which situations should clearly result in a breach of confidentiality? Which should not?
Which are debatable?

Grade differences can be reflected in the kind of information being kept confidential.

Confidentiality and keeping secrets is a hallmark of privacy, and students need to learn proper judgment about when to keep secrets and when not to. There are clear cases on each side, and there are cases in the gray zone. This is an area where judgment and guidance is needed. These gray cases are very hard, but students need to think about these cases and develop a good sense of judgment.

This lesson is probably too advanced for very young children, who should consult with their parents or teachers. Indeed, even older students might be encouraged to confide in others for advice such as teachers, school officials, or parents. These issues are very hard, and they sometimes might involve life-or-death consequences. Having guidance here can be very helpful for anyone. Indeed, it is recommended that schools have a designated official who can handle these issues and who can be known to students and all personnel at the school as the "go to" person to ask whenever in doubt. At many organizations, this person is the Privacy Officer, but any school official can fill this role if aware of the relevant laws and considerations.

Lesson: The goal of this activity is to teach students that betraying confidentiality can be an ethical violation. An important corollary lesson is that the value of keeping things confidential is not absolute. In some cases, students should be encouraged to breach confidentiality, such as when a student knows another has threatened violence or is contemplating suicide. Students should be taught that when in doubt, to reach out to people in positions to provide guidance such as teachers, school officials, or parents.

2. Online Disclosures

SHARING	K-3	4-8	9-12
Online disclosures	I treat others with respect online and in person. I explain why cyber- bullying is always wrong. I can identify the 3 different roles of a bullying encounter. I know what to do if I am the target or a bystander. I discuss how what I say about others is a reflection on me. I am honest.	I treat others with respect online and in person. I explain why cyber- bullying is always wrong and often illegal. I can identify the 3 different roles of a bullying encounter. I know what to do if I am the target or a bystander. I discuss how what I say about others is a reflection on me. I am honest. I understand the consequences of taking, sending, posting, or forwarding sexual images of a minor. (emotional, reputational, legal).	I treat others with respect online and in person. I explain why cyber- bullying is always wrong and often illegal. I can identify the 3 different roles of a bullying encounter. I know what to do if I am the target or a bystander. I discuss how what I say about others is a reflection on me. I am honest. I understand the consequences of taking, sending, posting, or forwarding sexual images of a minor or of an adult. (emotional, reputational, legal).

Various scenarios involving online disclosures. Some might involve disclosures made in a blog or on Facebook or Twitter. Other scenarios might be when a company discloses information about a person. Discuss: Which disclosures are appropriate? Which ones are troublesome or harmful?

Lesson: The goal of this activity is teach students why revealing information about others online can cause harm and be unwanted and unethical.

3. *Self-Exposure Online*

SHARING	K-3	4-8	9-12
Self exposure online	I cultivate a positive online reputation. I recognize that when I share online, I do not control who can see what I share.	I cultivate a positive online reputation. I recognize that when I share online, I do not control who can see what I share. I know that an internet or mobile message can last a long time, even ones that claim to be temporary or self- destructing. I know how to get help if I need something removed. I can locate the "report" buttons and I use them when I see something harmful or inappropriate online. I explain what types of disclosures are appropriate and desirable and what types might not be. Before sharing something online, I should PAUSE **P** - Do I have **Permission** to post this? (Is it mine to share?) **A** - Is it **Accurate**? (Is it true/honest?) **U** - Is it **Useful**? (Why am I posting this? Will it help others, teach others, **S** - Is it **Safe** to share? (Is it too personal/private/sexual? Is it legal?) **E** - Whose **Eyes** Will See it? (Am I ok with who will see this? Do I know who I am sharing this with)	I cultivate a positive online reputation. I recognize that when I share online, I do not control who can see what I share. I know that an internet post can last a long time, even ones that claim to be temporary or self-destructing. I know how to get help if I need something removed. I can locate the "report" buttons and I use them when I see something harmful or inappropriate online. I explain what types of disclosures are appropriate and desirable and what types might not be. Before sharing something online, I should PAUSE **P** - Do I have **Permission** to post this? (Is it mine to share?) **A** - Is it **Accurate**? (Is it true/honest?) **U** - Is it **Useful**? (Why am I posting this? Will it help others, teach others, **S** - Is it **Safe** to share? (Is it too personal/private/sexual? Is it legal?) **E** - Whose **Eyes** Will See it? (Am I ok with who will see this? Do I know who I am sharing this with)

Students role-play an employer or college admissions officer looking at an online profile of a character. Discuss: What would the employer / officer think? Should the information affect the decision?

Alternatively, students can examine an online profile of a character for what facts might be unwise to reveal. Students black out the facts that might be unwise. In later grades, students can evaluate the profile and identify the risks that disclosing various pieces of information can create.

Video vignette demonstrating the consequences of exposing data online.

Lesson: The goal of this activity is to teach students to understand the consequences when they expose data about themselves online. A video vignette can demonstrate the point, but a very effective way to do this is

through role-playing. Students need to see how things look from perspectives outside their own. Putting themselves in the role of an employer or admissions officer forces them to see things from a new perspective.

Students should be encouraged to Google themselves to make sure that they know what others can find out about them online. We recommend, though, that any activity involving real individuals not be done in a live classroom setting, as embarrassing or sensitive data might turn up.

THE IKEEPSAFE PILLARS

1. Balance

Balance: Maintaining a healthy balance between online and offline activities.

For privacy, balance involves taking advantage of the benefits of technology and also safeguarding personal information. In the online environment especially, various websites and new technological tools facilitate greater sharing of information. Some such sites actively encourage sharing. On some sites and services, it may the extent of data that is collected may not be readily apparent, and students may not fully realize just how much data they are sharing.

Additionally, students often have distorted perceptions about how much they share in the online environment, and they often feel differently when revealing information online as opposed to offline. Disclosing data online feels like a solitary activity and the full extent of the disclosure is often not appreciated. Would students disclose the same amount of data to a crowded auditorium? It is far easier to disclose sensitive information when one doesn't see thousands of faces staring back at him or her.
Removing this physical perception makes it harder to cognitively assess the consequences of disclosure. True, students may know intellectually that their disclosures online might be exposed to the world, but they might not feel it because the online environment strips away much of the sensory input that would shape the way they feel.

People say things online that they would never say in face-to-face, which can destabilize relationships. The lack of visual cues from the listener may contribute to the speaker saying something or speaking in a way that he/she might not when they can observe the listener's response. In addition, the belief that their comments are anonymous may embolden the speaker to be mean or to use a harsher persona than if their identity was known.

Thus the online environment can be destabilizing, upsetting the balance that exists offline for what people say about themselves and what they say about others. Students need to learn how to establish this balance in the online environment where they lack the same kind of physical cues and sensory input that exists offline.

2. Ethical Use

Ethical Use: Making ethical decisions, being considerate of others and understanding consequences of online behavior.

Many privacy violations are unethical. Although a number of cases of breaching confidentiality and gossiping might not be illegal, they are viewed by many as unethical. Why are they unethical? Because they are a violation of trust. Breaching confidentiality is essentially breaking a promise or betraying a friend. Gossip can be unethical too, because it can harm other people. Much gossip is done for personal pleasure or for social status, not for any truly compelling reason. When weighed against the consequences to the person who is gossiped about, the ethics come more into focus: The gossiper cares more about himself or herself than hurting other people.

Other privacy violations are unethical too. Peeping (sometimes called "creeping") and prying into people's private lives is a form of unwanted intrusion. It is failing to show respect for another person. Failing to respect other people's information boundaries is also a form of disrespect. An analogy might be made to kicking down another person's sandcastle that the other person spent a long time building. People work very carefully to establish their boundaries; invading them or destroying them ruins the hard work and time that people put into maintaining these boundaries.

Of course, cyberbullying, video voyeurism, and revenge porn are clearly unethical.

3. Privacy

Privacy: Protecting personal information and that of others.

Privacy involves respecting your own boundaries around what and how much information you share, and the boundaries of others. To protect their own privacy, students must understand some of the ways that personal data is collected and used. They should understand that "free" online services are not always really free, and they should understand that these services may be offered without payment in exchange for collection of their data. They should familiarize themselves with the terms of service and privacy policy before they start using online services and sharing information.

4. Relationships

Relationships: Engaging in safe and healthy online connections.

Students have many different types of relationships – with their closest friends, acquaintances, parents, teachers, siblings, employers, and boyfriends or girlfriends. Each type of relationship has certain boundaries and involves certain information that is shared and other information that is concealed.
Privacy is a key way people regulate and structure these relationships.

For relationships, privacy involves respecting other people's information boundaries. Violations of these boundaries – breaches of confidentiality, gossip, taking and sharing photos without consent, snooping, etc. – can severely damage or destroy personal relationships. Many friendships are impaired or ruined by privacy violations. Privacy in the form of boundaries serves a key function in social relationships because there is a lot of friction in life. Good boundaries help people live in a more tranquil, less anxious way.

Additionally, stranger danger involves relationships too, and students need to learn to be careful when forging relationships online.

5. Reputation

Reputation: Building a positive and truthful online reputation that will contribute to future success.

One's reputation is a very valuable asset and must be cultivated and treated with care. A good reputation can be very helpful in making new friends, finding employment, getting admitted into schools, and much more. A bad reputation can close doors and constrain opportunities.

In addition to one's own reputation, privacy also involves respecting the reputation of others. People have a right to not have falsehoods and lies spread about them. People also have a right to keep certain information concealed. This latter right is more complicated because it isn't absolute. There are times when a person's desire to conceal information should be outweighed by other considerations. But there are many times when a person's desire to conceal information should be respected.

People have varying levels of privacy expectations – while people may enjoy sharing their vacation photos; the others on the vacation may not want that information circulated. In addition, people may wish to keep information private to protect themselves from hasty and unfair judgments, from hypocrisy, from others condemning them based on only part of the story, or from being misunderstood.

6. Online Security

Online Security: Using good habits for securing hardware and software.

Privacy and online security go hand-in-hand. Data security will not be effective if the data isn't kept private. So the most elaborate safe can be built to protect a diary. There should be a comprehensive approach to protecting data that involves both privacy and security. Often, security is thought of as a technical issue. It is to some extent. But a significant dimension of good security involves good practices, such as selecting good passwords, keeping passwords private, encrypting data, avoiding putting data on devices where it can readily be lost or stolen, and understanding how to spot a phishing attempt.

Acknowledgements

We would like to thank the many educators and privacy experts that contributed to the iKeepSafe Privacy Curriculum Matrix K-12 BEaPRO™. Specifically, we'd like to thank Professor Daniel Solove for his substantial contribution to the privacy concepts outlined in the matrix and Francis Yasharain for aligning these concepts with age appropriate goals, objectives, and education approach. The input and expertise of advisory board members ensured that the recommendations outlined in this matrix are comprehensive and effective.